Generalized Sidon Sets

Carlos Vinuesa

Directed by Javier Cilleruelo

Generalized Sidon Sets

by

Carlos Vinuesa del Río

Thesis Advisor

Francisco Javier Cilleruelo Mateo

Departamento de Matemáticas

Facultad de Ciencias

Universidad Autónoma de Madrid

October, 2009

Preface

Welcome to the real world.

The Matrix

Take a set of integers, say $A = \{1, 2, 3, 4\}$, and calculate all the possible sums of two elements of the set: $A + A = \{2, 3, 4, 5, 6, 7, 8\}$. If you give me the sum 5 then I can not deduce if you have picked 1 and 4 or 2 and 3. Now take a different set, say $S = \{1, 2, 4, 8\}$, and again calculate all the possible sums of two of its elements: $S + S = \{2, 3, 4, 5, 6, 8, 9, 10, 12, 16\}$. If you give me the sum 8 I know that you picked 4 twice, if you give me 10 I know that you picked 2 and 8, and the same thing happens with every possible sum. S is a Sidon set.

In other words, A is a Sidon set if all the sums a_1+a_2, $a_i \in A$, are different (except when they coincide because of conmutativity, $a_1 + a_2 = a_2 + a_1$). If we pick 5 numbers in arithmetic progression, there will be a lot of repeated sums and they will not form a Sidon set. On the other hand, if we pick 5 numbers at random, between say 1 and 100, very probably they will form a Sidon set. So constructing Sidon sets is not difficult. The interesting thing is constructing Sidon sets with as many elements as we can.

We can consider infinite sets instead of finite ones (we will call them sequences instead of sets). We can allow 5 repetitions of each sum instead of only one. We can add up seven elements instead of two. In any case, our goal will be to give bounds for the number of elements a generalized Sidon set can have. In our way, we will find interesting constructions, combinatorics, probability, analysis...

Welcome to the exciting world of Sidon sets.

Table of Contents

Acknowledgements

It is nice to be important, but it
is more important to be nice.
Unknown

From time to time we have the oportunity to thank the worthwhile people that we have around us. Of course, we have to seize these opportunities.

Quiero agradecer, en primer lugar, a Javier, porque todo esto es sin duda gracias a él. En tiempos en los que aparentar y hablar están a la orden del día, es extraordinario comprobar que hay gente que sigue predicando con el ejemplo. Su trabajo es una motivación.

I want to thank Andrew Granville for showing me, among other things, that there is an easy proof for everything. I want to thank all the people that made my stay in Montreal so pleasant, specially Tristan (for the time we shared), and Grant, Derrick, Marc and Sophie-Anne (for the magic).

Vull agraïr a tota la gent que varen fer tant agradables les meves estades a Barna, especialment al Juanjo, a l'Itziar, al Luis Pedro, al Juan Pablo, a l'Ondra, al Tomas, a l'altre Tomas, al Hoang, al Paulius, al Laurence, al Benjamin, al Gonzalo i al Simon. I al Oriol Serra per la organització dels cursets de combinatòria i per ser sempre tan amable. També vull agraïr a tots els mags que m'han fet passar tants bons moments a Catalunya, i molt especialment al Isaac i al Toni Looser, dels que he aprés molt i encara més m'he rigut amb ells.

Szeretnék köszönetet mondani Ruzsa Imrének, amiért olyan nagyszerűen megmutatta hogyan lehet egy problémát természetesen, okosan és ügyesen

megközelíteni és hogy lehetőséget adott arra, hogy belássam: egy zseni is követ el hibákat és megakad néha-néha. Köszönet a sziporkázó humoráért, a kedvességéért, a teákért és a csokikért valamint az intenzív magyar nyelvleckékért.

Ezúton mondanék köszönetet Matolcsi Máténak a lényegretöréséért és amiért megmutatta, hogy néha jobb azonnal nekikezdeni a dolgoknak, mind hosszasan eltöprengeni rajtuk.

Szeretnék köszönetet mondani továbbá Balogh Antalnak és kedves feleségének, Annának, a vendégszeretetükért és nagyszerű együtt töltött pillanatokért.

Köszönet azoknak az embereknek, akik segítettek, hogy a Budapesten eltöltött idő oly nagyszerűen telt. Külön köszönet Istvánnak, aki lehetővé tette hogy mindvégig nála lakhassak, és aki eme sorokat lefordította erre a csodálatos nyelvre.

Je veux remercier Olivier Ramaré pour sa sympathie, son amabilité et son hospitalité. Et aussi pour son cours sur les cribles.

నూర్యరమణ గారికి మరియు వారి నుకుటుంబ నభ్యల అతిథీ నత్కరమునకు నేను వారికి హ్రుదయవూర్వకంగా ధన్యవాదములు తెలియచేనుకుంటున్నాను.

मैं ज्ञान प्रकाश और उनकी पत्नी जानव्ही का अतिथि संस्कार के लिये धन्यवाद करना चाहता हूँ।

Quero agradecer ao Manuel Silva, por todas as conversas, pelos seus conselhos, pela motivação que me deu, por me incentivar a ser melhor matemático e pelo seu sentido de humor, sobretudo pelas nossas piadas privadas ("isto tem de sair") e por todas as coisas divertidas que nos aconteceram nas nossas viagens pelo mundo.

Gracias a todos los profesores (no es preciso que llene esta línea con motes), algunos de matemáticas y otros no, que en algún momento me motivaron. Gracias a toda la gente de la Olimpiada Matemática, con una

especial dedicatoria a María Gaspar por la motivación y por las clases de problemas. Y gracias a Miguel de Guzmán por aquel curso en Santander. Gracias a todos los colaboradores y lectores de "La hoja volante". Gracias a todos mis alumnos.

Muchas gracias al "frikiteam" al completo. A Ana por ser como una madre y por su buen criterio para todo, a Pablo que constituye en todos los aspectos un ejemplo a seguir, a Mari Luz por su apoyo y su ánimo incondicional y a Angélica por ser como es, por su ayuda en tantas cosas, por entenderme siempre y por tener solución para todo. Y a Angélica otra vez por avisarme de todo (si no fuera por ti me habrían echado ya de la universidad seguramente...).

Quiero dar las gracias a todos los miembros del departamento. Especialmente a Eugenio Hernández y Ana Bravo, por su trabajo incansable, su cercanía y su apoyo. Agradezco a Fernando Chamizo todo su apoyo y su trabajo, su disponibilidad, su integridad y todo lo que me ha enseñado, además de sus geniales apuntes y otras tantísimas cosas. Gracias a Antonio Córdoba por recibirme siempre con una sonrisa aunque sea para pedirle firmas o dinero, y por iniciar la corriente de teoría de los números en el departamento. También quiero hacer un agradecimiento especial a Pepe García-Cuerva por su amabilidad y ayuda y por el curso de Matemática Discreta. Quiero agradecer a Cris, Paloma y Antonio su simpatía, su apoyo y su trabajo. En cuanto a los "jóvenes" (espero no dejarme a nadie), gracias a Elías (por sus ánimos, su sentido del humor y la serenidad que siempre aporta), Charro (por su liderazgo, sus irónicos y tronchantes comentarios y su cercanía), Alberto (por las escapadas en bicicleta), Alessandro (por las cervezas compartidas), Fernando, Jose, Ernesto, Enrique y Marijose (observad que os he incluido en jóvenes, por ser tan majetes y por vuestro apoyo), Nati (por tener siempre una respuesta divertida), Javi (por su particular y calmado punto de vista y su sentido del humor), Moisés (por su humor "friki"), David Lee (por su humor más "friki" todavía), Stinga (por sus boludeces, el fútbol, el volley, la piscina...), Adrián (por todo, tendría que hacer un capítulo sólo para darte las gracias), Elena (por su alegría y su

apoyo), Dani (el "güey", por su serenidad y su humor: "¡Quieto Rayo!"), Ana (por su optimismo y su entusiasmo), Sofía (por su simpatía y amabilidad), Roberto (por la olimpiada, por el fútbol y por esos conciertos), Edu (por el fútbol y sus conversaciones y monólogos), Sara (por sus ayudas con ordenadores, flexicubos y demás y por su dulzura) y Johanna (por su confianza y su cercanía y por todos los ánimos). Doy las gracias de modo muy especial a mis compañeros de despacho Boumediane (que aunque ya no está aquí fue un ejemplo en mis comienzos), Ibraheem (por no perder nunca la sonrisa y por su apoyo), Pablo (por su hospitalidad, su ayuda con los ordenadores, su integridad y su sentido del humor) y Pedro "er carvo" (por ser un "peligrozo" entrañable, por su cercanía y por esas conversaciones que mantenemos de vez en cuando).

Apartado especial merecen los siguientes amigos, magos y maleantes, que si bien no tuvieron mucho que ver de modo directo con esta tesis, estuvieron siempre ahí durante todo este tiempo. Gracias a Jaime y Vero (y a Manoli y Jaime que siempre nos acogen tan bien), a Corro y a toda la gente de Pucela por todos los grandes momentos vividos. Gracias a Luis y Mónica, Paco y Rut, Sergio y Ainel y Diego por tantos momentos y experiencias compartidas y por estar siempre ahí. Gracias a la casualidad, a Pablo (sí, el mismo del "frikiteam") y a Vicente Canuto por abrirme las puertas de este increíble mundo que es la magia y que ocupa bastante parte del tiempo que no dedico a las matemáticas (y parte del que sí les dedico). Gracias a todos los grandes magos de los que tanto he aprendido a través de libros, conferencias, actuaciones, vídeos y personalmente. Gracias a todos los profesores de la escuela de los que tanto aprendí y sigo aprendiendo: Ricardo (la pureza, la integridad y el respeto), Gea (la locura, la expresividad, la fuerza del momento y la originalidad), Miguel Gómez (la profundidad y la grandeza), Furni (la personalidad y la finura), Llaser (el cariño, la simpatía y la malvadez), Ramón (el ingenio y la practicidad), Alberto (la sencillez y la comunicación) y Óscar (la cercanía y la suavidad). Gracias a Juan, por los comienzos. Gracias a Rafa, por los comienzos, por su generosidad, lo que hemos vivido y lo que nos quedará... Gracias a los magos de Tres Cantos, Pablo, Ana, Iñaki y Jose (¡y a Conchi!) por cenas, congresos y nervios com-

partidos. Gracias a todos los amigos de la SEI, de modo muy muy especial a Miguel Ajo (por ser un ejemplo, por tanta inspiración, por sus consejos y por sus enseñanzas, directas o desprendidas de sus actuaciones), a Manolo Talman (por las "quedadas piscineras" y por tantas anécdotas), a Jose ("que es él", por su pureza e integridad, por todo lo aprendido de él y por hacerme experimentar la sensación de imposibilidad) y a Woody (por sus libros, por sus consejos, por sus ánimos y por su cercanía). A Miguel Muñoz y a Felipe por todo lo que hemos compartido y su personal estilo. Um agradecimento especial ao Helder, pela sua proximidade e por tudo o que aprendi com ele, pessoalmente e através do seu livro. Gracias a Germán, por las matemáticas, las magias y las tonterías compartidas. Gracias a Pacho por las magias y anécdotas compartidas. Gracias a Jacobo por su imborrable sonrisa, su simpatía, su sentido del humor, su apoyo y su magia. Gracias a Cris por todos los momentos, por las fotos, por las risas, por la motivación y por todo. Gracias a Fer por tantísimas cosas graciosas y raras (menos las de los camareros). Gracias a Michael Díaz por risas, viajes, momentos y conversaciones compartidas (y también por algunas magias). Eeeeefectivamente, gracias a Rober por su entusiasmo, por estar siempre ahí, ya sea para dar ánimos o para llevar la contraria, y por ser tan "crack". Gracias a Cristina por no echar muchas broncas a Alberto por no usar posavasos ni a mí por arrastrar cosas y por recibirnos siempre con una sonrisa. Muchas gracias a Alberto, por ser tan genial, tan familiar, tan trabajador, tan original, tan motivador, tan inspirador y tan cercano: "Maestro, eso no es botón derecho, ¡eso es darle a la manivela!". Gracias a Roci y a toda la familia de Pablo, que siempre me hacen sentir como en casa, especialmente a Luis, que es un figura, por las anécdotas y las risas. Y, como no podía ser de otra manera, muchísimas gracias a Pablo por pensar siempre lo mismo al mismo tiempo, por las innumerables horas de risas, por todas las actuaciones, todos los ensayos y todas las ideas, por acordarse siempre de todo, por ver mis fallos y disculparlos (eh, eh, que yo también disculpo los suyos...) y por permitirse el lujo de aprender algo de mí al tiempo que yo aprendo tanto de él. Y como diría el gran Frakson, gracias a todos los públicos, pues ellos hacen que esto merezca la pena.

Gracias a toda mi familia. En especial a mis tíos Enrique y Jaime, por su ejemplo y motivación. Por último, las más sinceras gracias a mi padre, que quizá tenga mucho que ver en todas las cosas que me gustan, a mi madre, que quizá tenga mucho que ver en todas las cosas que hago, y a mi hermano, que quizá tenga mucho que ver en que intente hacerlas todas lo mejor posible.

Part I

Generalized Sidon Sequences

Chapter 1

The Probabilistic Method

Las cosas más triviales
se vuelven fundamentales,
eliminando los moldes del azar.
Opio, Héroes del Silencio

As the quotation[1] suggests, the Probabilistic Method is a simple but very powerful tool.

The basic method can be described as follows (see [1]): if we want to prove the existence of a combinatorial structure with certain properties, we can construct an appropiate probability space and show that a randomly chosen element in this space has the desired properties with positive probability. As simple as "if something happens with positive probability it is because it happens sometime". Observe that the contrary is not neccesarily true: there are things that happen and have probability zero.

Despite its apparent simplicity, it is true that at first sight it could look surprising that calculating probabilities can prove facts with certainty. Well, even if it is hard to believe it, not only it works, but it happens many times that the best way to prove the existence of an element with certain properties is showing that "the probability of all the elements with this properties is positive". Furthermore, in many occasions this probability will be one or very close to one.

We will see this better with some examples.

[1] *The most trivial things become fundamental, removing the chance molds.* Opium, Heroes of the Silence.

As we said in the preface, A is a Sidon set if all the sums $a_1 + a_2$, $a_i \in A$, are different (except when they coincide because of conmutativity). As a warm-up, we start with a "finite" example. We fix N and we will use the probabilistic method to prove the existence of "large" Sidon sets in the inteval of integers $\{1, 2, \ldots, N\}$.

We start by taking a random subset A of $\{1, 2, \ldots, N\}$, with the property that $\mathbb{P}(i \in A) = p$, independently for every $i \in \{1, 2, \ldots, N\}$, where $0 < p < 1$ is a real number that we will fix later.

Then, the expected value of the number of elements of A is

$$\mathbb{E}(|A|) = Np$$

and its variance

$$\mathbb{V}(|A|) = Np(1-p).$$

The well known Chebyshev's inequality[2] says that

$$\mathbb{P}(||A| - Np| \geq 2\sqrt{Np(1-p)}) \leq \frac{1}{4}.$$

In other words, $|A| > Np - 2\sqrt{Np(1-p)}$ with probability greater than or equal to $3/4$.

What is the probability of A not being a Sidon set? We first fix n and write the probability of n having two or more representations as a sum of two elements of A

$$\mathbb{P}(n \text{ has 2 or more representations}) = \mathbb{P}\left(\bigcup_{\substack{\{(x,y),(z,t)\} \\ x+y=z+t=n \\ x\leq y, z\leq t}} ((x,y),(z,t) \in A^2) \right)$$

[2] **Chebyshev's Inequality.** If X is any real random variable with finite variance, σ^2, then for every real number $k > 0$: $\mathbb{P}(|X - \mathbb{E}(X)| \geq k\sigma) \leq \frac{1}{k^2}$.

and since the probability of the union is less than or equal to the sum of the probabilities, this is

$$\leq \sum_{\substack{\{(x,y),(z,t)\} \\ x+y=z+t=n \\ x\leq y, z\leq t}} \mathbb{P}((x,y),(z,t) \in A^2).$$

If (x,y) and (z,t) share an element then they must be equal, so the only possible repetition is that of $(n/2, n/2)$ in the same pair. This means that the last sum is

$$= \sum_{\substack{\{(x,y),(z,t)\} \\ x+y=z+t=n \\ x<y, z<t}} \mathbb{P}((x,y),(z,t) \in A^2) + \sum_{\substack{\{(x,y),(z,t)\} \\ x+y=z+t=n \\ x=y, z<t}} \mathbb{P}((x,y),(z,t) \in A^2).$$

For the first sum, we have n possibilities for x and, once we have chosen x, we have less than n possibilities for z. The values of y and t are determined by x and z. For the second sum, $x = y$ are determined, we have n possibilites for z and t is determined once we have chosen z. Remember also that the probability $\mathbb{P}(i \in A) = p$, independently for every i. All this means that our two sums are

$$\leq n^2 p^4 + np^3.$$

Bearing in mind that the sum of two elements of $\{1, 2, \ldots, N\}$ is less than or equal to $2N$,

$$\begin{aligned} \mathbb{P}(A \text{ is not Sidon}) &\leq \sum_{n=1}^{2N} (n^2 p^4 + np^3) \\ &\leq 2N((2N)^2 p^4 + 2Np^3) \\ &= 8N^3 p^4 + 4N^2 p^3. \end{aligned}$$

Since we are interested only in large values of N (we said that N is fixed, but we are thinking that it is big), we can impose the condition $2Np \geq 1$

and then

$$\mathbb{P}(A \text{ is not Sidon}) \leq 8N^3p^4 + 4N^2p^3 = 8N^3p^4\left(1 + \frac{1}{2Np}\right) \leq 16N^3p^4.$$

And here is the last "trick". So far we know that

$$\mathbb{P}(|A| > Np - 2\sqrt{Np(1-p)}) \geq 3/4 \quad \text{and} \quad \mathbb{P}(A \text{ is Sidon}) \geq 1 - 16N^3p^4.$$

We want the two things to happen at the same time in order to have a large Sidon sequence. Well, $\mathbb{P}(A_1 \cup A_2) = \mathbb{P}(A_1) + \mathbb{P}(A_2) - \mathbb{P}(A_1 \cap A_2)$, so the probability of the two things happening at the same time is $\mathbb{P}(A_1 \cap A_2) = \mathbb{P}(A_1) + P(A_2) - \mathbb{P}(A_1 \cup A_2) \geq \mathbb{P}(A_1) + \mathbb{P}(A_2) - 1$. If $\mathbb{P}(A_1) + \mathbb{P}(A_2) > 1$ we are done, since we have with possitive probability the two things at the same time. This means that we have to impose

$$3/4 + 1 - 16N^3p^4 > 1 \Rightarrow p < \left(\frac{3}{64}\right)^{1/4} N^{-3/4}.$$

In short, choosing $p < \left(\frac{3}{64}\right)^{1/4} N^{-3/4}$ and $N \geq 1/2p$, with positive probability we will have that A is a Sidon set with more than $Np - 2\sqrt{Np(1-p)}$ elements. In other words, for large N we will have[3]

$$|A| \gg N^{1/4}.$$

This is not by any means the best density we can obtain ($\gg N^{1/2}$ is the "correct" bound, see Chapter 3), but this method has the advantage that it

[3]Whenever we do not know the exact form of a quantity or we only want to get an idea of its size, we use the next notations from Landau:

- "$f(x) = o(g(x))$ when $x \to a$" means $\lim_{x\to a} \frac{|f(x)|}{|g(x)|} = 0$
- "$f(x) = O(g(x))$ when $x \to a$" means $\limsup_{x\to a} \frac{|f(x)|}{|g(x)|} = C < \infty$ (yes, a o is also a O)

Vinogradov's notation "$f(x) \ll g(x)$ when $x \to a$" means the same as "$f(x) = O(g(x))$ when $x \to a$". Observe that $f \ll g$ does not imply $f \leq g$.

Most of the times our a will be ∞. We will employ the more convenient notation, depending on the situation.

can be extended to the infinite case.

It is the perfect moment to go into a more interesting (infinite!) example that is completely related with the next chapter, but first we should introduce some notation.

Given an integer $h \geq 2$, we say that a sequence of positive integers A is a $B_h[g]$ sequence[4] if every integer n has at most g representations as a sum of h elements of A (where we consider equal two representations if they have the same elements in a different order). We will write

$$r_{h,A}(n) = |\{(a_1, a_2, \ldots, a_h) \mid n = a_1 + \cdots + a_h, \quad a_1 \leq \cdots \leq a_h, \quad a_i \in A\}|,$$

and then A is $B_h[g]$ if and only if $r_{h,A}(n) \leq g$ for every n. As usual, $A(x) = |A \cap [1, x]|$ counts the number of elements of A less than or equal to x.

In 1960, Erdős, the initiator of the probabilistic method, and Rényi ([12]) proved

Theorem 1.0.1. *For any $\varepsilon > 0$ there exists $g = g(\varepsilon)$ and a $B_2[g]$ sequence, A, such that $A(x) \gg x^{1/2-\varepsilon}$.*

Proof. Now we consider the random sequence A of positive integers defined by $\mathbb{P}(x \in A) = x^{-\alpha}$, where $0 < \alpha < 1$ will be fixed later. Then it is true that with probability 1, $A(x) \gg x^{1-\alpha}$ when $x \to \infty$ (see Theorem 2.3.2). Now

$$\mathbb{P}(r_{2,A}(n) \geq g+1) = \mathbb{P}\left(\bigcup_{\substack{\{(x_1,y_1),\ldots,(x_{g+1},y_{g+1})\} \\ x_i \leq y_i,\ x_i + y_i = n}} ((x_1, y_1), \ldots, (x_{g+1}, y_{g+1}) \in A^2) \right)$$

and since the probability of the union is less than or equal to the sum of the probabilities, this is

[4]The "B" probably coming from the word "bounded". And yes! a $B_2[1]$ sequence is a Sidon sequence.

$$\leq \sum_{\substack{\{(x_1,y_1),\dots,(x_{g+1},y_{g+1})\} \\ x_i \leq y_i,\ x_i+y_i=n}} \mathbb{P}((x_1,y_1),\dots,(x_{g+1},y_{g+1}) \in A^2).$$

Now observe that again if two of the pairs, say (x_i, y_i) and (x_j, y_j), share one element then, since $x_i + y_i = x_j + y_j = n$, they must share also the other element and $(x_i, y_i) = (x_j, y_j)$. Since our sum is on different pairs, we know that the events $((x_i, y_i) \in A^2)$ and $((x_j, y_j) \in A^2)$ are independent. This independence is crucial and we will not have it for $h \geq 3$. As we will see, it is necessary to use some new ideas to settle this matter for $h \geq 3$. Then, the last formula is

$$= \sum_{\substack{\{(x_1,y_1),\dots,(x_{g+1},y_{g+1})\} \\ x_i \leq y_i,\ x_i+y_i=n}} \mathbb{P}((x_1,y_1) \in A^2) \cdots \mathbb{P}((x_{g+1},y_{g+1}) \in A^2)$$

which is

$$\leq \left(\sum_{\substack{(x,y) \\ x \leq y,\ x+y=n}} \mathbb{P}((x,y) \in A^2) \right)^{g+1}.$$

The largest element of every pair is $y \geq n/2$, so this is

$$\leq \left(\left(\frac{n}{2}\right)^{-\alpha} \left(1 + \sum_{x<n/2} x^{-\alpha} \right) \right)^{g+1},$$

where the one before the sum comes from the case $x = y = n/2$ (if it is possible). Finally, using that $\sum_{x<n/2} x^{-\alpha} \leq c_\alpha n^{1-\alpha}$ for a constant c_α depending only on α (the sum is close to the integral $\int_0^{n/2} x^{-\alpha} dx$), we have

$$\mathbb{P}(r_{2,A}(n) \geq g+1) \leq C_\alpha n^{(1-2\alpha)(g+1)}.$$

We want $(1-2\alpha)(g+1) < -1$ in order to use Borel-Cantelli Lemma[5] and prove that, with probability 1, $r_{2,A}(n) \geq g+1$ happens only a finite number of times.

Then, for every $\alpha > \frac{1}{2} + \frac{1}{2g+2}$, with probability 1 we can remove a finite number of elements from A to have a $B_2[g]$ sequence[6].

This removal does not affect to the density of A, so we can finally state: Given $\varepsilon > 0$, for any $g > \frac{1}{2\varepsilon} - 1$, with probability 1 we can remove a finite number of elements from A to have a $B_2[g]$ sequence with density $\gg x^{1/2-\varepsilon}$. □

We observe that not only we prove the existence of one sequence satisfiying our desired properties as the theorem says, but also that from a randomly chosen sequence in our probability space, with probability 1 we can remove a finite number of elements to have a sequence that satisfy these properties. So "most of the sequences" satisfy what we want, but we are unable to exhibit one. That's life!

Erdős and Rényi claimed (but did not prove) that the same method gives the analogous result for $h \geq 2$:

Theorem 1.0.2. *For any $\varepsilon > 0$ and $h \geq 2$, there exists $g = g_h(\varepsilon)$ and a $B_h[g]$ sequence, A, such that $A(x) \gg x^{1/h-\varepsilon}$.*

Probably they didn't notice that when $h \geq 3$ two distinct representations of an integer as a sum of h numbers can share common elements. If $x_1 + \cdots + x_h = y_1 + \cdots + y_h$ and $x_1 = y_1$, then the events $(x_1, \ldots, x_h \in A)$ and $(y_1, \ldots, y_h \in A)$ are not independent.

In [33] Vu gave the first correct proof of Theorem 1.0.2. He used ideas from a paper of Erdős (ironically, he solved his own troubles) and Tetali to

[5] **Borel-Cantelli Lemma.** Let $(E_n)_{n=1}^{\infty}$ be a sequence of events in a probability space. If $\sum_{n=1}^{\infty} \mathbb{P}(E_n) < \infty$ then the probability that infinitely many of them occur is 0.

[6] Of course, if two things happen with probability one, its union also happens with probability one (very easy since $\mathbb{P}(A_1 \cup A_2) = \mathbb{P}(A_1) + \mathbb{P}(A_2) - \mathbb{P}(A_1 \cap A_2)$).

solve a similar problem for a related question. The key point is the use of the Sunflower Lemma[7] to prove that if an integer has enough representations then we can select $g+1$ representations which are disjoint. Now the probabilistic method works easily because we deal with independent events. If we follow the details of the proof we can see that Vu obtains $g_h(\varepsilon) \ll \varepsilon^{-h+1}$.

The use of the Sunflower Lemma is an ingenious idea and it do solve the "absence of independence problem". But the relation between g and ε, $g_h(\varepsilon) \ll \varepsilon^{-h+1}$, apparently leaves room for improvement. In the next chapter we will gather together some notations and ideas to try to improve this relation. We will also give a constructive proof of Theorem 1.0.2. Finally, using the "alteration method", we will try to give a sharper bound for the particular case $h = 3$.

[7] A collection of sets (multisets) $A_1, \ldots, A_r$ is a sunflower if the sets (multisets) have pairwise the same intersection (it can be empty).

Sunflower Lemma. If H is a collection of sets (multisets) of size at most k and $|H| > (r-1)^k k!$ then H contains r sets (multisets) forming a sunflower.

Chapter 2

Generalized Sidon Sequences

A man ceases to be a beginner in any given science and becomes a master in that science when he has learned that he is going to be a beginner all his life.

Robin G. Collingwood

The work of this chapter is a joint work with Javier Cilleruelo, Sándor Z. Kiss and Imre Z. Ruzsa [7].

2.1 Introduction

Remember from Chapter 1 that a sequence of positive integers A is a $B_h[g]$ sequence if $r_{h,A}(n) \leq g$ for every positive integer n, where

$$r_{h,A}(n) = |\{(a_1, a_2, \ldots, a_h) \mid n = a_1 + \cdots + a_h, \quad a_1 \leq \cdots \leq a_h, \quad a_i \in A\}|.$$

Remember also that $A(x) = |A \cap [1, x]|$, the number of elements of A less than or equal to x. The counting method easily gives $A(x) \ll x^{1/h}$ for any $B_h[g]$ sequence[8]. It is believed that a $B_h[g]$ sequence A can not satisfy $A(x) \gg x^{1/h}$. However it is only known when $(h, g) = (\text{even}, 1)$.

In a seminal paper, Erdős and Rényi [12] proved, using the probabilistic method, that for any $\varepsilon > 0$ there exists $g = g(\varepsilon)$ and a $B_2[g]$ sequence such that $A(x) \gg x^{1/2-\varepsilon}$ (see Chapter 1). In this paper they claimed (but

[8] $A \in B_h[g] \Rightarrow A(x)^h \leq h! \sum_{n \leq hx} r_{h,A}(n) \leq h! hgx \Rightarrow A(x) \ll x^{1/h}$.

did not prove) that the same method gives the analogous result for $h \geq 3$ (Theorem 1.0.2), probably because they did not realize of the "absence of independence problem", a phenomena which makes the cases $h \geq 3$ much more difficult than the case $h = 2$. In [33] Vu gave the first correct proof of Theorem 1.0.2, using the Sunflower Lemma and obtaining $g_h(\varepsilon) \ll \varepsilon^{-h+1}$ (see again Chapter 1).

Our aim is to present new proofs of Theorem 1.0.2 and to obtain better relations between g and ε.

In Section 2.2 we give an explicit construction of the sequence claimed in Theorem 1.0.2.

In Section 2.3 we give a probabilistic but distinct and simpler proof than that presented by Vu. We do not use the Sunflower Lemma, but a simpler one, and we get a better upper bound for $g_h(\varepsilon)$. More precisely, we prove the next theorem in Section 2.3:

Theorem 2.1.1. *For any $\varepsilon > 0$ and $h \geq 2$, there exists $g = g_h(\varepsilon) \ll \varepsilon^{-1}$ and a $B_h[g]$ sequence, A, such that $A(x) \gg x^{1/h-\varepsilon}$.*

Actually we can check in the proof of the theorem above that we can take any $g_h(\varepsilon) \geq 2^{h-3}h(h-1)!^2\varepsilon^{-1}$. The improvement of this theorem affects to the cases $h \geq 3$, where we have to deal with not independent events. Vu's proof only gives $g_h(\varepsilon) \ll \varepsilon^{-h+1}$ which is worse than our bound when $h \geq 3$. For the case $h = 2$ Erdős and Rényi proved that any $g_2(\varepsilon) > \frac{1}{2\varepsilon} - 1$ satisfies the condition of Theorem 2.1.1 and Cilleruelo [5] used the "alteration method" to improve that bound to $g_2(\varepsilon) > \frac{1}{4\varepsilon} - \frac{1}{2}$.

In Section 2.4 we refine Theorem 2.1.1 when $h = 3$, proving that $g_3(\varepsilon) > \frac{2}{9\varepsilon} - \frac{2}{3}$ works. In other words,

Theorem 2.1.2. *For every $\varepsilon > 0$ and for every $g \geq 1$ there is a $B_3[g]$ sequence A, such that*

$$A(x) \gg x^{\frac{g}{3g+2}-\varepsilon}.$$

It is also possible to refine Theorem 2.1.1 for $h \geq 4$ using the "alteration method" but the exponents we would obtain in these cases are not satisfactory enough. For "satisfactory enough" we mean exponents such that when we particularize to $g = 1$, we obtain the same exponent that we get with the greedy algorithm[9]. That is what happens for $h = 2$ ([5]) and $h = 3$ (Theorem 2.1.2).

2.2 A constructive proof

Given h and ε, we construct a sequence A with $r_{h,A}(n)$ bounded and we will prove that $A(n) > n^{1/h-\varepsilon}$ for sufficiently large n, which implies Theorem 1.0.2.

We use the representation of natural numbers in a number system with variable base. It is easy to see that every natural number x can be expressed uniquely in the form

$$x = b_0 + b_1 q_1 + b_2 q_1 q_2 + \cdots + b_s q_1 \cdots q_s + \cdots ,$$

where $0 \leq b_i < q_{i+1}$. The b_i's and q_i's are natural numbers, b_i's called the "digits" and q_i's called the "bases".

We consider $l \geq 2$, a large enough number that will be fixed later. We fix the sets $0 \in A_i \subseteq \left[0, \frac{q_i}{h}\right]$ such that the A_i's are maximal sets with the condition $r_{h,A_i}(n) \leq 1$ for every n. Now we construct the set A in the following way: put that natural numbers in A which digits $b_i \in A_{i+1}$, and for which there is an m such that $b_i = 0$ for $i \notin [m+1, \ldots, m+l]$.

First we prove that $r_{h,A}(n) < (h!)^{lh}$. We add up h numbers, a_1, a_2, ..., a_h.

[9] One way for obtaining a Sidon sequence (i. e. a $B_2[1]$ sequence) is using the well known "greedy algorithm". Briefly, we construct the sequence $A = \{a_1, a_2, a_3, \ldots\}$ inductively: we take $a_1 = 1$ and, once we have chosen $a_1, a_2, \ldots, a_{m-1}$ forming a Sidon set, a_m is the least positive integer different from $a_r + a_s - a_t$ with $1 \leq r, s, t \leq m-1$. This sequence A has $A(x) \gg x^{1/3}$. We can make the obvious generalization to obtain a $B_h[1]$ sequence A, with $A(x) \gg x^{1/(2h-1)}$.

Since the j-th digit of each addend is in $\left[0, \frac{q_j}{h}\right]$, each digit of the sum will be the sum of the j-th digits of the a_i's (in other words, there will be no carries).

And, since the j-th digit of each addend is in a $B_h[1]$ set, the j-th digit of the sum can be obtained in only one way as a sum of h digits. Note that h numbers have $h!$ permutations, so for each digit of the sum we could have the corresponding digits of the h addends distributed in at most $h!$ ways.

Finally, observe that the sum of the number of non zero digits of all the addends is less than or equal to hl, so the number of digits of the sum different from zero will also be less than or equal to hl, and finally we will have $r_{h,A}(n) \leq (h!)^{lh}$ for every n.

Now, we give an estimation of the value of $A(n)$. Given n, we know that there exists j such that

$$q_1 q_2 \cdots q_j \leq n < q_1 q_2 \cdots q_{j+1}. \tag{2.1}$$

It is clear that those integers which digits

$$b_0 = b_1 = \cdots = b_{j-l-1} = 0 \ \text{ and } \ b_i \in A_{i+1}, \ i = j-l, \ldots, j-1,$$

are in A. Let N denote the number of such integers. We define $r = \dfrac{\log_2 l}{l}$. Let $q_1 = \lfloor e \rfloor = 2$ and

$$q_i = \lfloor e^{(1+r)^{i-1}} \rfloor. \tag{2.2}$$

We know (Bose-Chowla[10]; see, for example, [17]) that

$$|A_i| > \frac{1}{2}\left(\frac{q_i}{h}\right)^{1/h}. \tag{2.3}$$

Since $\frac{e^{(1+r)^{i-1}}}{2} \leq q_i \leq e^{(1+r)^{i-1}}$ and $2(2h)^{1/h} \leq 2e^{2/e} < e^2$ we have

[10]The result of Bose and Chowla implies that for every q which is a power of a prime, and for every $h \geq 2$ there is a set $C = \{c_1, \ldots, c_q\} \subseteq [0, q^h - 1)$ with $r_{h,C}(n) \leq 1$. Combining this result with the well known Bertrand's postulate (for every integer $n \geq 2$ there is a prime $p \in (n, 2n)$) we can assure that (2.3) is satisfied.

$$|A_i| > \frac{1}{2}\left(\frac{e^{(1+r)^{i-1}}}{2h}\right)^{1/h} > e^{\frac{(1+r)^{i-1}}{h}-2} \tag{2.4}$$

First we give an upper bound for $\log n$. It follows from (2.1) and (2.2) that

$$\log n < \log(q_1 \cdots q_{j+1}) \leq 1 + (1+r) + \cdots + (1+r)^j < \frac{(1+r)^{j+1}}{r}. \tag{2.5}$$

In the next step we will give a lower estimation for $\log N$. Applying (2.4) we have

$$\begin{aligned} \log N = \sum_{i=j-l+1}^{j} \log|A_i| &> \frac{(1+r)^{j-l} + \cdots + (1+r)^{j-1}}{h} - 2l \\ &= \frac{(1+r)^j}{hr}(1-(1+r)^{-l}) - 2l. \end{aligned} \tag{2.6}$$

In view of (2.5) and (2.6) we have

$$\begin{aligned} \frac{h\log N}{\log n} &> \frac{(1+r)^j(1-(1+r)^{-l})}{(1+r)^{j+1}} - \frac{2lrh}{(1+r)^{j+1}} \\ &= \frac{1-(1+r)^{-l}}{1+r} - \frac{2lrh}{(1+r)^{j+1}}. \end{aligned} \tag{2.7}$$

Using that $\frac{1}{1+r} > 1-r$ and that $\left(1+\frac{\log_2 l}{l}\right)^{\frac{l}{\log_2 l}} \geq 2$ for any $l \geq 2$, we have

$$\begin{aligned} \frac{1-(1+r)^{-l}}{1+r} &> 1-r-(1+r)^{-l} = 1 - \frac{\log_2 l}{l} - \left(1+\frac{\log_2 l}{l}\right)^{-l} \\ &> 1 - \frac{\log_2 l}{l} - \frac{1}{l} > 1 - \frac{2\log_2 l}{l}. \end{aligned} \tag{2.8}$$

On the other hand, since $\lim_{j\to\infty} \frac{2lrh}{(1+r)^{j+1}} = 0$ we have that, for sufficiently large j,

$$\frac{2lrh}{(1+r)^{j+1}} < \frac{\log_2 l}{l}. \tag{2.9}$$

Finally, from (2.7), (2.8) and (2.9) we have

$$\frac{h \log N}{\log n} > 1 - \frac{3 \log_2 l}{l},$$

for sufficiently large n.

We finish the proof of Theorem 1.0.2 taking, for a given $\varepsilon > 0$, a large enough integer l such that $\frac{3 \log_2 l}{l} < h\varepsilon$, because then $\log N > \left(\frac{1}{h} - \varepsilon\right) \log n$, i. e. $N > n^{1/h-\varepsilon}$.

Just a little comment about the dependence of g on ε. Observe that our g is $(h!)^{lh}$ and that, given ε, we need to choose a large value of l, say $l \gg \varepsilon^{-1} \log \varepsilon^{-1}$. This makes the dependence of g on ε very bad. The value of g we get with this construction depends more than exponentially on ε^{-1}. We will try to improve this in the next section and, for the case $h = 3$, even more in the last one.

Note that in [6] we can find an explicit Sidon sequence with $A(x) \gg x^{1/3-o(1)}$. But this construction can not be generalized.

2.3 A new probabilistic proof

Definition 2.3.1. Given $0 < \alpha < 1$ we define $S(\alpha, m)$ as the probability space of the sequences of positive integers defined by

$$P(x \in A) = \begin{cases} 0 & \text{if } x < m \\ x^{-\alpha} & \text{if } x \geq m \end{cases}.$$

Theorem 2.3.2. *For any m, a random sequence A in $S(\alpha, m)$ satisfies $A(x) \gg x^{1-\alpha}$ with probability 1.*

Proof. First of all, we calculate

$$\mathbb{E}(A(x)) = \sum_{n \leq x} \mathbb{P}(n \in A) = \sum_{m \leq n \leq x} n^{-\alpha} = \frac{x^{1-\alpha}}{1-\alpha} + O_{\alpha,m}(1),$$

when $x \to \infty$. Now, we use Chernoff's Lemma[11] to get

$$\begin{aligned}\mathbb{P}\left(A(x) \leq \tfrac{1}{2}\mathbb{E}\left(A(x)\right)\right) &\leq \mathbb{P}\left(|A(x) - \mathbb{E}(A(x))| \geq \tfrac{1}{2}\mathbb{E}(A(x))\right) \\ &\leq 2e^{-\frac{1}{16}\left(\frac{x^{1-\alpha}}{1-\alpha}+O(1)\right)}.\end{aligned}$$

Since $\sum_{x=1}^{\infty} 2e^{-\frac{1}{16}\left(\frac{x^{1-\alpha}}{1-\alpha}+O(1)\right)} < \infty$, Borel-Cantelli Lemma[12] says that $A(x) \gg x^{1-\alpha}$ with probability 1. □

Notation 2.3.3. We denote the set which elements are the coordinates of the vector $\bar{x}$ as $Set(\bar{x})$. Of course, if two or more coordinates of $\bar{x}$ are equal, this value appears only once in $Set(\bar{x})$.

Notation 2.3.4. We define

$$R_h(n) = \{(n_1, n_2, \ldots, n_h) \mid n = n_1 + \cdots + n_h, \quad n_1 \leq \cdots \leq n_h, \quad n_i \in \mathbb{N}\}.$$

Lemma 2.3.5. *For a sequence A in $S(\alpha, m)$, for every h and n*

$$\mathbb{E}(r_{h,A}(n)) \leq C_{h,\alpha}\ n^{h(1-\alpha)-1}$$

where $C_{h,\alpha}$ depends only on h and α.

Proof.

$$\begin{aligned}\mathbb{E}(r_{h,A}(n)) &= \sum_{\bar{x}\in R_h(n)} \prod_{x\in Set(\bar{x})} \mathbb{P}(x \in A) \\ &= \sum_{j=1}^{h} \sum_{\substack{\bar{x}\in R_h(n) \\ |Set(\bar{x})|=j}} \prod_{x\in Set(\bar{x})} \mathbb{P}(x \in A).\end{aligned}$$

[11] Let $X = t_1 + \cdots + t_n$ where the t_i are independent Boolean random variables. **Chernoff's Lemma** says that for every $0 < \varepsilon < 2$, $\mathbb{P}(|X - \mathbb{E}(X)| \geq \varepsilon\mathbb{E}(X)) \leq 2e^{-\varepsilon^2\mathbb{E}(X)/4}$. See Lemma 3.6.3.

[12] Please find Borel-Cantelli Lemma in a footnote of Chapter 1.

Since the largest element of every $\bar{x} \in R_h(n)$ is $\geq n/h$ we have

$$\begin{aligned}
\mathbb{E}(r_{h,A}(n)) &\leq \left(\frac{n}{h}\right)^{-\alpha} \sum_{j=1}^{h} \left(\sum_{x<n} x^{-\alpha}\right)^{j-1} \\
&\leq \left(\frac{n}{h}\right)^{-\alpha} \sum_{j=1}^{h} \left(\int_0^n x^{-\alpha}\, dx\right)^{j-1} \\
&\leq \left(\frac{n}{h}\right)^{-\alpha} \sum_{j=1}^{h} \left(\frac{n^{1-\alpha}}{1-\alpha}\right)^{j-1} \\
&\leq C_{h,\alpha}\, n^{h(1-\alpha)-1}.
\end{aligned}$$

□

Definition 2.3.6. We say that two vectors $\bar{x}$ and $\bar{y}$ are disjoint if $Set(\bar{x})$ and $Set(\bar{y})$ are disjoint sets. We define $r^*_{l,A}(n)$ as the maximum number of pairwise disjoint representations of n as sum of l elements of A, i. e. the maximum number of pairwise disjoint vectors of $R_l(n)$ with their coordinates in A. We say that A is a $B^*_l[g]$ sequence if $r^*_{l,A}(n) \leq g$ for every n.

Lemma 2.3.7. *For a sequence A in $S(\alpha, m)$, for every h and n*

$$\mathbb{P}(r^*_{h,A}(n) \geq s) \leq C_{h,\alpha,s}\, n^{(h(1-\alpha)-1)s}$$

where $C_{h,\alpha,s}$ depends only on h, α and s.

Proof. Using the independence given by the pairwise disjoint condition

$$\begin{aligned}
\mathbb{P}(r^*_{h,A}(n) \geq s) &= \sum_{\substack{\{\bar{x}_1,\ldots,\bar{x}_s\} \\ \bar{x}_i \in R_h(n) \\ \bar{x}_1,\ldots,\bar{x}_s \\ \text{pairwise disjoint}}} \prod_{i=1}^{s} \prod_{x \in Set(\bar{x}_i)} \mathbb{P}(x \in \mathcal{A}) \\
&\leq \left(\sum_{\bar{x} \in R_h(n)} \prod_{x \in Set(\bar{x})} \mathbb{P}(x \in \mathcal{A})\right)^s
\end{aligned}$$

$$= \quad E(r_{h,A}(n))^s$$

and using Lemma 2.3.5 we conclude the proof. □

Proposition 2.3.8. *Given $h \geq 2$ and $0 < \varepsilon < 1/h$, a random sequence in $S(1 - \frac{1}{h} + \varepsilon, m)$ is a $B_h^*[g]$ sequence for every $g \geq \frac{2}{h\varepsilon}$ with probability $1 - O(\frac{1}{m})$.*

Proof. From Lemma 2.3.7, and taking into account the value of $\alpha = 1 - \frac{1}{h} + \varepsilon$, we have

$$\mathbb{P}(r_{h,A}^*(n) \geq g + 1) \leq C_{h,\varepsilon,g} n^{-h\varepsilon(g+1)}.$$

Since $r_{h,A}^*(n) = 0$ for $n < m$ we have

$$\begin{aligned} \mathbb{P}\left(r_{h,A}^*(n) \geq g + 1 \text{ for some } n\right) &\leq \sum_{n \geq m} \mathbb{P}\left(r_{h,A}^*(n) \geq g + 1\right) \\ &\leq \sum_{n \geq m} C_{h,\varepsilon} n^{-h\varepsilon(g+1)}. \end{aligned}$$

If $g \geq \frac{2}{h\epsilon}$, the last sum is $O(1/m)$. Thus, if it is the case,

$$\begin{aligned} \mathbb{P}\left(r_{h,A}^*(n) \leq g \text{ for every } n\right) &= 1 - \mathbb{P}\left(r_{h,A}^*(n) \geq g + 1 \text{ for some } n\right) \\ &\geq 1 - O\left(\frac{1}{m}\right). \end{aligned}$$

□

The next "simple" lemma is the key idea of the proof of Theorem 2.1.1.

Lemma 2.3.9.

$$B_h^*[g] \cap B_{h-1}[k] \subseteq B_h[hkg].$$

Remark 2.3.10. In fact, the "true" lemma, which is a little more ugly, is

$$B_h^*[g] \cap B_{h-1}[k] \subseteq B_h[g(h(k-1)+1)]$$

and this is what we will prove. As an example, we can have in mind that a sequence A with $r^*_{3,A}(n) \leq g$ which is a Sidon sequence is also a $B_3[g]$ sequence, i. e. $B^*_3[g] \cap B_2[1] \subseteq B_3[g]$, since in this case two representations that share one element share the three of them.

Proof. We proceed by contradiction. Suppose that $A \in B^*_h[g] \cap B_{h-1}[k]$ and suppose that there is an n with $g(h(k-1)+1)+1$ distinct representations as a sum of h elements of A.

Fix one of these representations, say $n = x_1 + x_2 + \cdots + x_h$. How many representations of n can intersect with it? Well, the number of representations of n that involve x_1 is at most k, since $A \in B_{h-1}[k]$. So we have at most $k-1$ more representations with x_1. The same thing happens for $x_2, \ldots, x_h$. So, finally, the maximun number of representations that can intersect with the one we fixed is $h(k-1)$.

Now we fix a second representation of n that does not intersect with the first one that we chose. Again, there are at most $h(k-1)$ representations that intersect with our new choice.

After g disjoint choices, counting them and all the representations that intersect with each one of them, we have at most $gh(k-1)+g$ representations. By hipothesis, there is at least one representation of n left that does not intersect with any of our g choices. But this means that we have $g+1$ disjoint representations of n, which contradicts the fact that $A \in B^*_h[g]$. □

Proposition 2.3.11. *For every $h \geq 2$ and $0 < \varepsilon < 1/h$ a random sequence in $S(1 - \frac{1}{h} + \varepsilon, m)$ is a $B_h[g]$ sequence for every $g \geq c_h/\varepsilon$ with probability $1 - O(\frac{1}{m})$, where $c_h = 2^{h-3}h(h-1)!^2$.*

Proof. We proceed by induction on h.

For $h = 2$, and using Proposition 2.3.8, the result is true since a $B^*_2[g]$ sequence is the same that a $B_2[g]$ sequence.

Now suppose that the result is true for $h-1$. Let $\alpha = 1 - \frac{1}{h} + \varepsilon$. From Proposition 2.3.8 we know that a random sequence in $S(\alpha, m)$ is $B_h^*[g_1]$ for every $g_1 \geq \frac{2}{h\varepsilon}$ with probability $1-O(\frac{1}{m})$. But, since $\alpha > 1-\frac{1}{h-1}+\frac{1}{h(h-1)}$, by the induction hypothesis we know that this random sequence is also $B_{h-1}[g_2]$ for every $g_2 \geq h(h-1)c_{h-1} = c_h/2$ with probability $1 - O(\frac{1}{m})$. So, with probability $1 - O(\frac{1}{m})$ the two things happen at the same time, i. e. the random sequence is in $B_h^*[g_1] \cap B_{h-1}[g_2]$ for every $g_1 \geq \frac{2}{h\varepsilon}$ and $g_2 \geq c_h/2$.

Lemma 2.3.9 concludes the proof. □

Lemma 2.3.2 and Proposition 2.3.11 imply Theorem 2.1.1.

2.4 Sequences with $r_{3,A}(n)$ bounded

Now[13], we will try to find a more precise relation between g and ε. In fact, the result of Erdős and Rényi in [12] is more precise than what we said in the Introduction. They proved that for every $g > \frac{1}{2\varepsilon} - 1$ there is a $B_2[g]$ sequence, A, with $A(x) \gg x^{1/2-\varepsilon}$. Stated perhaps in a more convenient way, what they proved is that for every positive integer g there is a sequence A such that $r_{2,A}(n) \leq g$ with $A(x) \geq x^{\frac{1}{2+2/g}-o(1)}$, as $x \to \infty$.

In [5] Cilleruelo used the "alteration method" (perhaps our random sequences do not satisfy what we want but they do if we remove "a few" elements) to prove that for every $g > \frac{1}{4\varepsilon} - \frac{1}{2}$ there is a $B_2[g]$ sequence, A, with $A(x) \gg x^{1/2-\varepsilon}$. In other words, for every positive integer g there is a sequence A such that $r_{2,A}(n) \leq g$ with $A(x) \gg x^{\frac{1}{2+1/g}-o(1)}$ as $x \to \infty$.

In this section we will use the ideas from [5] to prove Theorem 2.1.2, which is a refinement on the dependence between g and ε, for sequences with $r_{3,A}(n) \leq g$.

[13] Of course, our Proposition 2.3.11 gives a relation between g and ε, but observe that for $g = 1$ it gives values of $\varepsilon \geq 1$, so it does not give any useful information. In our terminology, this is not a "satisfactory enough exponent".

Definition 2.4.1. Given a sequence of positive integers, A, we say that x is $(g+1)_h-$bad (for A) if $x \in A$ and there exist $x_1, \ldots, x_{h-1} \in A$, $x_1 \leq \cdots \leq x_{h-1} \leq x$, such that $r_{h,A}(x_1 + \cdots + x_{h-1} + x) \geq g+1$.

In other words, $x \in A$ is $(g+1)_h-$bad if it is the largest element in a representation of an element that has more than g representations as a sum of h elements of A. Observe that A is a $B_h[g]$ sequence if and only if it does not contain $(g+1)_h-$bad elements.

Definition 2.4.2. A sequence of positive integers, A, is in $\tilde{B}_h[g]$ if the number of $(g+1)_h-$bad elements less than or equal to x for A, say $\mathcal{B}(x)$, is

$$\mathcal{B}(x) = o(A(x)) \text{ when } x \to \infty.$$

So, $A \in \tilde{B}_h[g]$ if removing a few elements from it ("a little o"), it is a $B_h[g]$ sequence.

Notation 2.4.3. We denote by $\mathcal{B}_{k,h}(g+1)$ the set of $(g+1)_h-$bad elements for A in the interval $[h^k, h^{k+1})$.

Substituting $r_{h,A}$ by $r^*_{h,A}$, we define the $(g+1)^*_h-$bad elements for A. Analogously, we define $A \in \tilde{B}^*_h[g]$ and $\mathcal{B}^*_{k,h}(g+1)$

Obviously, the "tilde" version of Lemma 2.3.9 is also true. In particular, from Remark 2.3.10:

Lemma 2.4.4. $\tilde{B}^*_3[g] \cap \tilde{B}_2[1] \subseteq \tilde{B}_3[g]$.

Now we can write the next theorem, which we will use only in the cases $h = 2$ and $h = 3$.

Theorem 2.4.5. *Given* $0 < \delta < \frac{1}{2h-3}$ *and* $h \geq 2$, *a random sequence* A *in* $S\left(\frac{2h-4}{2h-3} + \delta, m\right)$ *is* $\tilde{B}^*_h[g]$ *for every* $g > \frac{\frac{h-1}{2h-3} - (h-1)\delta}{\frac{h-3}{2h-3} + h\delta}$ *with probability* $1 - O\left(\frac{1}{\log m}\right)$.

Proof. We consider a random sequence A in $S(\alpha, m)$.

$$\begin{aligned}
\mathbb{E}(|\mathcal{B}^*_{k,h}(g+1)|) &= \sum_{h^k \le x < h^{k+1}} \mathbb{P}(x \text{ is } (g+1)^*_h - \text{bad}) \\
&\le \sum_{h^k \le x < h^{k+1}} \sum_{\substack{\bar{x}_{g+1}=(y_1,\dots,y_{h-1},x) \\ y_1 \le \cdots \le y_{h-1} \le x}} \prod_{z \in Set(\bar{x}_{g+1})} \mathbb{P}(z \in A) \cdot \\
&\quad \cdot \sum_{\substack{\{\bar{x}_1,\dots,\bar{x}_g\} \\ \bar{x}_i \in R_h(y_1+\cdots+y_{h-1}+x) \\ \bar{x}_1,\dots,\bar{x}_g,\bar{x}_{g+1} \\ \text{pairwise disjoint}}} \prod_{i=1}^{g} \prod_{z \in Set(\bar{x}_i)} \mathbb{P}(z \in A) \\
&\le \sum_{h^k \le n < h^{k+2}} \left(\sum_{\bar{x} \in R_h(n)} \prod_{x \in Set(\bar{x})} \mathbb{P}(x \in A) \right)^{g+1} \\
&\le \sum_{h^k \le n < h^{k+2}} \left(C n^{h(1-\alpha)-1} \right)^{g+1} \\
&\ll \sum_{h^k \le n < h^{k+2}} n^{(h-1-h\alpha)(g+1)} \\
&\ll h^{k((h-1-h\alpha)(g+1)+1)}
\end{aligned}$$

when $k \to \infty$, where we have used Lemma 2.3.5.

Now, we can use Markov's Inequality[14] to have:

$$\mathbb{P}(|\mathcal{B}^*_{k,h}(g+1)| \ge k^2 \mathbb{E}(|\mathcal{B}^*_{k,h}(g+1)|)) \le \frac{1}{k^2}.$$

Since $|\mathcal{B}^*_{k,h}(g+1)| = 0$ for $h^{k+1} < m$ we have

$$\begin{aligned}
\mathbb{P}\left(|\mathcal{B}^*_{k,h}(g+1)| \ge k^2 \mathbb{E}(|\mathcal{B}^*_{k,h}(g+1)|) \text{ for some } k\right) &\le \sum_{k \ge \log_h m - 1} \frac{1}{k^2} \\
&= O\left(\frac{1}{\log m}\right),
\end{aligned}$$

[14] **Markov's Inequality.** For a random variable X and $a > 0$, $\mathbb{P}(|X| \ge a) \le \dfrac{\mathbb{E}(|X|)}{a}$.

so with probability $1 - O\left(\frac{1}{\log m}\right)$ we have that

$$|\mathcal{B}^*_{k,h}(g+1)| \ll k^2 h^{k((h-1-h\alpha)(g+1)+1)}$$

for every k.

On the other hand, by Theorem 2.3.2 we know that $A(x) \gg x^{1-\alpha}$ with probability 1.

So, given x, we will have $h^l \leq x < h^{l+1}$ for some l and with probability $1 - O\left(\frac{1}{\log m}\right)$ the number of bad elements less than or equal to x will be

$$\mathcal{B}(x) \leq \sum_{k=0}^{l} |\mathcal{B}^*_{k,h}(g+1)| \ll l^2 h^{l((h-1-h\alpha)(g+1)+1)}$$

while the number of elements in A less than or equal to x will be

$$A(x) \gg h^{l(1-\alpha)}.$$

Since, in order for A to be in $\tilde{B}^*_h[g]$, we want $\mathcal{B}(x) = o(A(x))$ we need

$$(h-1-h\alpha)(g+1)+1 < 1-\alpha$$

and so, with $\alpha = \frac{2h-4}{2h-3} + \delta$ we have

$$g > \frac{\frac{h-1}{2h-3} - (h-1)\delta}{\frac{h-3}{2h-3} + h\delta}.$$

□

In particular, for $h = 2$, since a $\tilde{B}^*_2[g]$ sequence is also a $\tilde{B}_2[g]$ sequence, we deduce that given $0 < \varepsilon < \frac{1}{3}$, a random sequence A in $S\left(\frac{2}{3} + \varepsilon, m\right)$ is $\tilde{B}_2[1]$ with probability $1 - O\left(\frac{1}{\log m}\right)$.

Also, for $h = 3$, we deduce that given $0 < \delta < \frac{1}{3}$, a random sequence A in $S\left(\frac{2}{3} + \delta, m\right)$ is $\tilde{B}_3^*[g]$ for every $g > \frac{2}{9\delta} - \frac{2}{3}$ with probability $1 - O\left(\frac{1}{\log m}\right)$.

Lemma 2.4.4 gives the proof of Theorem 2.1.2.

Part II

Generalized Sidon Sets

Chapter 3

Generalized Sidon Sets

I will not return to the United States while they maintain this policy in their airports.
And when they change it, I will have to think about another excuse.

Imre Z. Ruzsa

The work of this chapter is a joint work with Javier Cilleruelo and Imre Z. Ruzsa [9].

3.1 Introduction

A Sidon set A in a commutative group is a set with the property that the sums $a_1 + a_2$, $a_i \in A$, are all distinct except when they coincide because of commutativity. We will consider the case when, instead of that, a bound is imposed on the number of such representations. When this bound is g, these sets are often called $B_2[g]$ sets. Although in Part I we used this notation because it was more convenient, in this part we will prefer the terminology defined below, which is perhaps more respectful with "the origin of Sidon sets" (see Subsection 3.1.1). Observe that the generalization in this part is only on g, i. e. while we allow g to be greater than one, we will always be considering sums of only two addends.

Our main interest is in sets of integers and residue classes, but we formulate our concepts and some results in a more general setting.

Let G be a commutative group.

Definition 3.1.1. For $A \subseteq G$, we define the corresponding representation function[15] as

$$r(x) = |\{(a_1, a_2) : a_i \in A,\, a_1 + a_2 = x\}|.$$

The restricted representation function is

$$r'(x) = |\{(a_1, a_2) : a_i \in A,\, a_1 + a_2 = x,\, a_1 \neq a_2\}|.$$

Finally, the unordered representation function $r^*(x)$ counts the pairs (a_1, a_2) where (a_1, a_2) and (a_2, a_1) are identified[16]. With an ordering given on G (not necessarily in any connection with the group operation) we can write this as

$$r^*(x) = |\{(a_1, a_2) : a_i \in A,\, a_1 + a_2 = x,\, a_1 \leq a_2\}|.$$

These functions are not independent; we have always the equality

$$r^*(x) = r(x) - \frac{r'(x)}{2}$$

and the inequalities

$$r'(x) \leq r(x) \leq 2r^*(x).$$

We have $r(x) = r'(x)$ except for $x = 2a$ with $a \in A$. If we are in this last case and there are no elements of order 2 in G, then necessarily $r(x) = r'(x) + 1$. So, if there are no elements of order 2 in G the quantities are more closely connected:

$$r'(x) = 2\left\lfloor \frac{r(x)}{2} \right\rfloor,\ r^*(x) = \left\lceil \frac{r(x)}{2} \right\rceil.$$

This is the case in $\mathbb{Z}$, or in $\mathbb{Z}_q$ for odd values of q. For even q this is not

[15] Observe that from now on we will omit the subscripts in the representation functions: "the 2" because we will always be adding two elements and "the A" in order to relieve the notation (whenever it is clear the set we are talking about).

[16] Observe that the use of the word "unordered" is somewhat arbitrary. We can use "unordered" meaning that whatever the order of the elements of a pair is, it is considered the same representation. But we could also use "ordered" meaning that we consider ordered pairs, (a_1, a_2) with $a_1 \leq a_2$.

necessarily true, but both for constructions and estimates the difference seems to be negligible, as we shall see. In a group with lots of elements of order 2, like in $\mathbb{Z}_2^m$, the difference is substantial.

Definition 3.1.2. We say that A is a g-Sidon set, if $r(x) \leq g$ for all x. It is a weak g-Sidon set, if $r'(x) \leq g$ for all x. It is an unordered g-Sidon set, if $r^*(x) \leq g$ for all x.

Note 3.1.3. When we have a set of integers $C \subseteq [1, m]$, we say that it is a g-Sidon set $\pmod m$ if the residue classes $\{c \pmod m : c \in C\}$ form a g-Sidon set in $\mathbb{Z}_m$.

The strongest possible of these concepts is that of an unordered 1-Sidon set, and this is what is generally simply called a Sidon set. A weak 2-Sidon set is sometimes called a weak Sidon set.

These concepts are closely connected. If there are no elements of order 2, then $2k$-Sidon sets and unordered k-Sidon sets coincide[17], in particular, a 2-Sidon set is the same as a usual Sidon set. Also, in this case $(2k+1)$-Sidon sets and weak $2k$-Sidon sets coincide. Specially, a 3-Sidon set and a weak 2-Sidon set are the same.

Our aim is to find estimates for the maximal size of a g-Sidon set in an interval of integers or in a finite group.

3.1.1 The origin of the problem: g-Sidon sets in the integers

In 1932, the analyst Simon Sidon asked to a young Paul Erdős about the maximal cardinality of a g-Sidon set of integers in $\{1, \ldots, n\}$. Sidon was interested in this problem in connection with the study of the L_p norm of Fourier series with frequencies in these sets but Erdős was captivated by

[17] Observe also that an unordered k-Sidon set is the same as a $B_2[k]$ set. So, in the case that there are not elements of order 2 in G, our results for $2g$-Sidon sets will be results for $B_2[g]$ sets.

the combinatorial and arithmetical flavour of this problem and it was one of his favorite problems; not in vain it has been one of the main topics in Combinatorial Number Theory.

Definition 3.1.4. For a positive integer n

$$\beta_g(n) = \max\{|A| : A \subseteq \{1, \dots, n\},\ A \text{ is a } g\text{-Sidon set}\}.$$

We could define $\beta'_g(n)$ and $\beta^*_g(n)$ analogously.

The behaviour of this quantity is only known for classical Sidon sets and for weak Sidon sets : we have $\beta_2(n) \sim \sqrt{n}$ and $\beta_3(n) \sim \sqrt{n}$.

The reason which makes easier the case $g = 2$ is that 2-Sidon sets have the property that the differences $a - a'$ are all distinct. Erdős an Turán [14] used this to prove that $\beta_2(n) \leq \sqrt{n} + O(n^{1/4})$ and Lindström [19] refined that to get $\beta_2(n) \leq \sqrt{n} + n^{1/4} + 1$. For weak Sidon sets Ruzsa [28] proved that $\beta_3(n) \leq \sqrt{n} + 4n^{1/4} + 11$.

For the lower bounds, the classical constructions of Sidon sets of Singer [31], Bose [2] and Ruzsa [28] in some finite groups, $\mathbb{Z}_m$, give $\beta_3(n) \geq \beta_2(n) \geq \sqrt{n}(1 - o(1))$. Then, $\lim_{n\to\infty} \frac{\beta_2(n)}{\sqrt{n}} = \lim_{n\to\infty} \frac{\beta_3(n)}{\sqrt{n}} = 1$.

However for $g \geq 4$ it has not even been proved that $\lim_{n\to\infty} \beta_g(n)/\sqrt{n}$ exists. For this reason we write

$$\overline{\beta}_g = \limsup_{n\to\infty} \beta_g(n)/\sqrt{n} \qquad \text{and} \qquad \underline{\beta}_g = \liminf_{n\to\infty} \beta_g(n)/\sqrt{n}.$$

It is very likely that these limits coincide, but this has only been proved for $g = 2, 3$. A wide literature has been written with bounds for $\overline{\beta}_g$ and $\underline{\beta}_g$ for arbitrary g. The trivial counting argument[18] gives $\overline{\beta}_g \leq \sqrt{2g}$ while the strategy of pasting Sidon sets in $\mathbb{Z}_m$ in the obvious way[19] gives $\underline{\beta}_g \geq \sqrt{\lfloor g/2 \rfloor}$.

[18] If A is a g-Sidon set in $\{1, \dots, n\}$, then $|A|^2 = \sum_{N \leq 2n} r(N) \leq 2gn$, so $|A| \leq \sqrt{2gn}$.

[19] This will be better understood after reading Lemma 3.7.1. "The obvious way" means that A is a set of consecutive integers, $A = \{0, 1, 2, \dots, \lfloor g/2 \rfloor - 1\}$, which is obviously a $\lfloor g/2 \rfloor$-Sidon set.

The problem of narrowing this gap has attracted the attention of many mathematicians in the last years.

For example, while for $g = 4$ the trivial upper bound gives $\overline{\beta}_4 \leq \sqrt{8}$, it was proved in [4] that $\overline{\beta}_4 \leq \sqrt{6}$, which was refined to $\overline{\beta}_4 \leq 2.3635...$ in [26] and to $\overline{\beta}_4 \leq 2.3218...$ in [16].

On the other hand, Kolountzakis [18] proved that $\underline{\beta}_4 \geq \sqrt{2}$, which was improved to $\underline{\beta}_4 \geq 3/2$ in [8] and to $\underline{\beta}_4 \geq 4/\sqrt{7} = 1.5118...$ in [16].

We describe below the progress done in the last years:

$$\begin{aligned}
\tfrac{\overline{\beta}_g}{\sqrt{g}} &\leq \sqrt{2} = 1.4142... \text{ (trivial)} \\
&\leq 1.3180... \text{ (J. Cilleruelo - I. Z. Ruzsa - C. Trujillo, [8])} \\
&\leq 1.3039... \text{ (B. Green, [15])} \\
&\leq 1.3003... \text{ (G. Martin - K. O'Bryant, [22])} \\
&\leq 1.2649... \text{ (G. Yu, [34])} \\
&\leq 1.2588... \text{ (G. Martin - K. O'Bryant, [23])}
\end{aligned}$$

$$\begin{aligned}
\lim_{g\to\infty} \tfrac{\underline{\beta}_g}{\sqrt{g}} &\geq 1/\sqrt{2} = 0.7071... \text{ (M. Kolountzakis, [18])} \\
&\geq 0.75 \text{ (J. Cilleruelo - I. Z. Ruzsa - C. Trujillo, [8])} \\
&\geq 0.7933... \text{ (G. Martin - K. O'Bryant, [21])} \\
&\geq \sqrt{2/\pi} = 0.7978... \text{ (J. Cilleruelo - C. Vinuesa, [11]).}
\end{aligned}$$

Our main result connects this problem with a quantity arising from the analogous continuous problem, first studied by Schinzel and Schmidt [29]. Consider all nonnegative real functions f satisfying $f(x) = 0$ for all $x \notin [0, 1]$, and

$$\int_0^1 f(t)f(x-t)\,dt \leq 1$$

for all x. Define the constant σ by

$$\sigma = \sup \int_0^1 f(x)\,dx \tag{3.1}$$

where the supremum is taken over all functions f satisfying the above restrictions.

We will prove:

Theorem 3.1.5.

$$\lim_{g\to\infty} \frac{\underline{\beta}_g}{\sqrt{g}} = \lim_{g\to\infty} \frac{\overline{\beta}_g}{\sqrt{g}} = \sigma.$$

In other words, the theorem above says that the maximal cardinality of a g-Sidon set in $\{1,\dots,n\}$, $\beta_g(n)$, is:

$$\sqrt{gn}\ \underline{\sigma}(g)(1-\underline{\varepsilon}_g(n)) \le \beta_g(n) \le \sqrt{gn}\ \overline{\sigma}(g)(1+\overline{\varepsilon}_g(n)),$$

where $\underline{\sigma}(g)$ and $\overline{\sigma}(g) \to \sigma$ when $g \to \infty$ and, for a fixed value of g, $\underline{\varepsilon}_g(n)$ and $\overline{\varepsilon}_g(n) \to 0$ when $g \to \infty$.

Schinzel and Schmidt [29] and Martin and O'Bryant [23] conjectured that $\sigma = 2/\sqrt{\pi} = 1.1283...$, and an extremal function was given by $f(x) = 1/\sqrt{\pi x}$ for $0 < x \le 1$. But recently we have disproved it [24] with explicit functions f which give a greater value. The current state of the art for this constant is

$$1.1509... \le \sigma \le 1.2525...$$

both bounds coming from [24]. We will study this matter in Chapter 4.

The main difficulty in Theorem 3.1.5 is establishing the lower bound for $\lim \frac{\underline{\beta}_g}{\sqrt{g}}$. The upper bound, $\lim \frac{\overline{\beta}_g}{\sqrt{g}} \le \sigma$, proved in [11], is a direct application of a result of Schinzel and Schmidt from [29], as we will see in Section 3.5.

The usual strategy to construct large g-Sidon sets in the integers is pasting large Sidon sets modulo m in a suitable form. The strategy of pasting g-Sidon sets modulo m had not been tried before since there were no large enough known g-Sidon sets modulo m.

Precisely, the heart of the proof of Theorem 3.1.5 is the construction of large g-Sidon sets modulo m.

3.1.2 g-Sidon sets in finite groups

Definition 3.1.6. For a finite commutative group G write

$$\alpha_g(G) = \max\{|A| : A \subseteq G,\ A \text{ is a } g\text{-Sidon set}\}.$$

We could define $\alpha'_g(G)$ and $\alpha^*_g(G)$ analogously. For the cyclic group $G = \mathbb{Z}_q$, with an abuse of notation, we write $\alpha_g(q) = \alpha_g(\mathbb{Z}_q)$.

An obvious estimate[20] of this quantity is

$$\alpha_g(q) \leq \sqrt{gq}.$$

Our aim is to show that for large g, for some values of q this is asymptotically the correct value. More exactly, write

$$\alpha_g = \limsup_{q\to\infty} \alpha_g(q)/\sqrt{q}.$$

The case $g = 2$ (Sidon sets) is well known, we have $\alpha_2 = 1$. It is also known [28] that $\alpha_3 = 1$. Very little is known about α_g for $g \geq 4$.

For $g = 2k^2$, Martin and O'Bryant [21] generalized the well known constructions of Singer [31], Bose [2] and Ruzsa [28], obtaining $\alpha_g \geq \sqrt{g/2}$ for these values of g.

We are unable to exactly determine α_g for any $g \geq 4$, but we will find its asymptotic behaviour. Our main result sounds as follows.

Theorem 3.1.7. *We have*

$$\alpha_g = \sqrt{g} + O\left(g^{3/10}\right),$$

in particular,

$$\lim_{g\to\infty} \frac{\alpha_g}{\sqrt{g}} = 1.$$

[20] If A is a g-Sidon set in $\mathbb{Z}_q$, then $|A|^2 = \sum_{N\in\mathbb{Z}_q} r(N) \leq gq$, so $|A| \leq \sqrt{gq}$.

In Section 3.2, as a warm-up, we give a slight improvement of the obvious upper estimate.

In Section 3.3 we construct dense g-Sidon sets in groups $\mathbb{Z}_p^2$. In Section 3.4 we use this to construct g-Sidon sets modulo q for certain values of q.

Section 3.5 is devoted to the proof of the upper bound of Theorem 3.1.5. In Section 3.6, we connect the discrete and the continuous world, combining some ideas from Schinzel and Schmidt and some probabilistic arguments used in [11]. In Section 3.7 we prove the lower bound of Theorem 3.1.5 pasting copies of the large g-Sidon sets in $\mathbb{Z}_q$ which we constructed in Section 3.4 and using for that the sets obtained in Section 3.6.

3.2 An upper estimate

The representation function $r(x)$ behaves differently at elements of $2\cdot A = \{2a : a \in A\}$ and the rest; in particular, it can be odd only on this set. Hence we formulate our result in a flexible form that takes this into account.

Theorem 3.2.1. *Let G be a finite commutative group with $|G| = q$. Let $k \geq 2$ and $l \geq 0$ be integers and $A \subseteq G$ a set such that the corresponding representation function satisfies*

$$r(x) \leq \begin{cases} k, & \text{if } x \notin 2 \cdot A, \\ k + l, & \text{if } x \in 2 \cdot A. \end{cases}$$

We have

$$|A| < \sqrt{(k-1)q} + 1 + \frac{l}{2} + \frac{l(l+1)}{2(k-1)}. \tag{3.2}$$

Corollary 3.2.2. *Let G be a finite commutative group with $|G| = q$, and let $A \subseteq G$ be a g-Sidon set. If g is even, then*

$$|A| \leq \sqrt{(g-1)q} + 1.$$

If g is odd, then

$$|A| \leq \sqrt{(g-2)q} + \frac{3}{2} + \frac{1}{g-2}.$$

Indeed, these are cases $k = g$, $l = 0$ and $k = g-1$, $l = 1$ of the previous theorem.

Corollary 3.2.3. *Let $A \subseteq \mathbb{Z}_q$ be a weak g-Sidon set. If q is even, then*

$$|A| \leq \sqrt{(g-1)q} + 2 + \frac{3}{g-1}.$$

If q is odd, then

$$|A| \leq \sqrt{(g-1)q} + \frac{3}{2} + \frac{1}{g-1}.$$

To deduce this, we put $k = g$ and $l = 2$ if q is even, $l = 1$ if q is odd.

Proof. Write $|A| = m$. We shall estimate the quantity

$$R = \sum r(x)^2$$

in two ways.

First, observe that

$$r(x)^2 - kr(x) = r(x)\left(r(x) - k\right) \leq \begin{cases} 0, & \text{if } x \notin 2 \cdot A, \\ l(k+l), & \text{if } x \in 2 \cdot A, \end{cases}$$

hence

$$R \leq k \sum r(x) + l(k+l)\left|2 \cdot A\right|.$$

Since clearly $\sum r(x) = m^2$ and $|2 \cdot A| \leq m$, we conclude

$$R \leq km^2 + l(k+l)m. \tag{3.3}$$

Write

$$d(x) = |\{(a_1, a_2) : a_i \in A,\, a_1 - a_2 = x\}|.$$

Clearly $d(0) = m$. We also have $\sum d(x) = m^2$, and, since the equations $x + y = u + v$ and $x - u = v - y$ are equivalent,

$$\sum d(x)^2 = R.$$

We separate the contribution of $x = 0$ and use the inequality of the arithmetic and quadratic mean to conclude

$$R = m^2 + \sum_{x \neq 0} d(x)^2 \geq m^2 + \frac{1}{q-1} \left(\sum_{x \neq 0} d(x) \right)^2 > m^2 + \frac{m^2(m-1)^2}{q}.$$

A comparison with the upper estimate (3.3) yields

$$\frac{m^2(m-1)^2}{q} < (k-1)m^2 + l(k+l)m.$$

This can be rearranged as

$$(m-1)^2 < (k-1)q + \frac{l(k+l)q}{m}.$$

Now if $m < \sqrt{(k-1)q}$, then we are done; if not, we use the opposite inequality to estimate the second summand and we get

$$(m-1)^2 < (k-1)q + \frac{l(k+l)\sqrt{q}}{\sqrt{k-1}}.$$

We take square root and use the inequality $\sqrt{x+y} \leq \sqrt{x} + \frac{y}{2\sqrt{x}}$ to obtain

$$m - 1 < \sqrt{(k-1)q} + \frac{l(k+l)}{2(k-1)}$$

which can be written as (3.2). □

3.3 Construction in certain groups

In this section we construct large g-Sidon sets in groups $G = \mathbb{Z}_p^2$, for primes p. We shall establish the following result.

Theorem 3.3.1. *Given k, for every sufficiently large prime $p \geq p_0(k)$ there is a set $A \subseteq \mathbb{Z}_p^2$ with $kp - k + 1$ elements which is a g-Sidon set for $g = \lfloor k^2 + 2k^{3/2} \rfloor$.*

Observe that the trivial upper bound in this case is

$$|A| \leq \sqrt{gq} \leq kp\sqrt{1 + \frac{2}{\sqrt{k}}} < (k + \sqrt{k})p.$$

Proof. Let p be a prime. For every $u \not\equiv 0$ in $\mathbb{Z}_p$ consider the set

$$A_u = \left\{ \left(x, \frac{x^2}{u} \right) : x \in \mathbb{Z}_p \right\} \subseteq \mathbb{Z}_p^2.$$

Clearly $|A_u| = p$.

We are going to study the sumset of two such sets. For any $\underline{a} = (a, b) \in \mathbb{Z}_p^2$ we shall calculate the representation function

$$r_{u,v}(\underline{a}) = |\{(\underline{a}_1, \underline{a}_2) : \underline{a}_1 \in A_u, \underline{a}_2 \in A_v, \underline{a}_1 + \underline{a}_2 = \underline{a}\}|.$$

The most important property for us sounds as follows.

Lemma 3.3.2. *If $u+v \equiv u'+v'$ and $\left(\frac{uvu'v'}{p}\right) = -1$ then $r_{u,v}(\underline{a})+r_{u',v'}(\underline{a}) = 2$ for all $\underline{a} = (a, b) \in \mathbb{Z}_p^2$.*

Proof. If $a \equiv x+y$ and $b \equiv \frac{x^2}{u} + \frac{y^2}{v}$, with $uv \not\equiv 0$, then $y \equiv a-x$ and we have $b \equiv \frac{x^2}{u} + \frac{(a-x)^2}{v}$. We can rewrite this equation as $(u+v)x^2 - 2aux + ua^2 - buv \equiv 0$. The discriminant of this quadratic equation is $\Delta \equiv 4uv((u+v)b - a^2)$. The number of solutions is

$$r_{u,v}(a,b) = \begin{cases} 1 & \text{if } \left(\frac{\Delta}{p}\right) = 0 \\ 2 & \text{if } \left(\frac{\Delta}{p}\right) = +1 \quad (\Delta \text{ quadratic residue}) \\ 0 & \text{if } \left(\frac{\Delta}{p}\right) = -1 \quad (\Delta \text{ quadratic nonresidue}). \end{cases}$$

We can express this as

$$r_{u,v}(a,b) = 1 + \left(\frac{\Delta}{p}\right).$$

Now, since $u + v \equiv u' + v'$,

$$\begin{aligned} \Delta\Delta' &\equiv 4uv((u+v)b - a^2)4u'v'((u'+v')b - a^2) \\ &\equiv 16uvu'v'((u+v)b - a^2)^2 \end{aligned}$$

and we have

$$\begin{aligned} \left(\frac{\Delta}{p}\right)\left(\frac{\Delta'}{p}\right) &= \left(\frac{\Delta\Delta'}{p}\right) = \left(\frac{uvu'v'}{p}\right)\left(\frac{((u+v)b-a^2)^2}{p}\right) \\ &= -\left(\frac{((u+v)b-a^2)^2}{p}\right) \end{aligned}$$

because $\left(\frac{uvu'v'}{p}\right) = -1$.

If $(u+v)b - a^2 \equiv 0$, we have $\left(\frac{\Delta}{p}\right) = \left(\frac{\Delta'}{p}\right) = 0$. If not, we have $\left(\frac{\Delta}{p}\right)\left(\frac{\Delta'}{p}\right) = -1$. In any case get

$$\left(\frac{\Delta}{p}\right) + \left(\frac{\Delta'}{p}\right) = 0.$$

□

We resume the proof of the theorem.

We put

$$A = \bigcup_{u=t+1}^{t+k} A_u.$$

and we will show that for a suitable choice of t this will be a good set.

Since $(0,0) \in A_u$ for all u and the rest of the A_u's are disjoint, we have $|A| = k(p-1)+1$.

We can estimate the corresponding representation function as

$$r(\underline{a}) \leq \sum_{u,v=t+1}^{t+k} r_{u,v}(\underline{a})$$

(equality fails sometimes, because representations involving $(0,0)$ are counted once on the left and several times on the right).

We parametrize the variables of summation as $u = t+i, v = t+j$ with $1 \leq i,j \leq k$. So $2 \leq i+j \leq 2k$ and we can write $i+j = k+1+l$ with $|l| \leq k-1$.

For fixed l, we have $k-|l|$ pairs i,j (which means $k-|l|$ pairs u,v). These pairs can be split into two groups: n^+ of them will have $\left(\frac{uv}{p}\right) = 1$ and n^- will have $\left(\frac{uv}{p}\right) = -1$. Clearly

$$n^+ + n^- = k - |l|,\ n^+ - n^- = \sum \left(\frac{uv}{p}\right).$$

Of these $n^+ + n^-$ pairs we can combine $\min\{n^+, n^-\}$ into pairs of pairs with opposite quadratic character, that is, with $\left(\frac{uvu'v'}{p}\right) = -1$. For these we use Lemma 3.3.2 to estimate the sum of the corresponding representation functions $r_{u,v} + r_{u',v'}$ by 2. For the uncoupled pairs we can only estimate the individual values by 2. Altogether this gives

$$\sum_{i+j=k+1+l} r_{u,v}(\underline{a}) \quad \leq \quad 2(\min\{n^+,n^-\}) + 2(\max\{n^+,n^-\} - \min\{n^+,n^-\})$$

$$\begin{aligned} &= 2(\max\{n^+, n^-\}) \\ &= n^+ + n^- + |n^+ - n^-| \\ &= k - |l| + \left|\sum \left(\frac{uv}{p}\right)\right|. \end{aligned}$$

Adding this for every possible value of l, for a fixed t we obtain

$$r(\underline{a}) \leq k^2 + \sum_{|l|\leq k-1} \left| \sum_{i+j=k+1+l} \left(\frac{(t+i)(t+j)}{p}\right)\right| = k^2 + S_t.$$

We are going to show that S_t is small on average. Since we need values with $u, v \not\equiv 0$, we can use only $0 \leq t \leq p-1-k$; however, the complete sum is easier to work with. Applying the Cauchy-Schwarz inequality we get

$$\begin{aligned} \sum_{t=0}^{p-1} S_t &= \sum_{t,l} \left| \sum_{i+j=k+1+l} \left(\frac{(t+i)(t+j)}{p}\right)\right| \\ &\leq \sqrt{2kp \sum_{l,t} \left(\sum_{i+j=k+1+l} \left(\frac{(t+i)(t+j)}{p}\right)\right)^2} \\ &\leq \sqrt{2kp \sum_{i+j=i'+j'} \sum_{t} \left(\frac{(t+i)(t+j)(t+i')(t+j')}{p}\right)}. \end{aligned}$$

To estimate the inner sum we use Weil's Theorem that asserts

$$\left|\sum_{t=0}^{p-1} \left(\frac{f(t)}{p}\right)\right| \leq \deg f \sqrt{p}$$

for any polynomial f which is not a constant multiple of a square. Hence

$$\sum_{t=0}^{p-1} \left(\frac{(t+i)(t+j)(t+i')(t+j')}{p}\right) \leq 4\sqrt{p}$$

except when the numerator as a polynomial of t is a square.

The numerator will be a square if the four numbers i, i', j, j' form two equal pairs. This happens exactly $k(2k-1)$ times. Indeed, we may have $i = i'$, $j = j'$, k^2 cases, or $i = j'$, $j = i'$, another k^2 cases. The k cases when all four coincide have been counted twice. Finally, if $i = j$ and $i' = j'$, then the equality of sums implies that all are equal, so this gives no new case. In these cases for the sum we use the trivial upper estimate p.

The total number of quadruples i, i', j, j' is $\leq k^3$, since three of them determine the fourth uniquely.

Combining our estimates we obtain

$$\sum_{t=0}^{p-1} S_t \leq \sqrt{2p^2k^2(2k-1) + 8p^{3/2}k^4}.$$

This implies that there is a value of t, $0 \leq t \leq p-k-1$ such that

$$S_t \leq \frac{\sqrt{2p^2k^2(2k-1) + 8p^{3/2}k^4}}{p-k} < 2k^{3/2}$$

if p is large enough. This yields that $r(\underline{a}) < k^2 + 2k^{3/2}$ as claimed. □

3.4 Construction in certain cyclic groups

In this section we show how to project a set from $\mathbb{Z}_p^2$ into $\mathbb{Z}_q$ with $q = p^2 s$.

Theorem 3.4.1. *Let $A \subseteq \mathbb{Z}_p^2$ be a g-Sidon set with $|A| = m$, and put $q = p^2 s$ with a positive integer s. There is a g'-Sidon set $A' \subseteq \mathbb{Z}_q$ with $|A'| = ms$ and $g' = g(s+1)$.*

Proof. An element of A is a pair of residues modulo p, which we shall represent by integers in $[0, p-1]$. Given an element $(a, b) \in A$, we put into A' all numbers of the form $a + cp + bsp$ with $0 \leq c \leq s-1$. Clearly $|A'| = sm$.

To estimate the representation function of A' we need to tell, given a, b, c, how many $a_1, b_1, c_1, a_2, b_2, c_2$ are there such that

$$a + cp + bsp \equiv a_1 + c_1 p + b_1 sp + a_2 + c_2 p + b_2 sp \pmod{p^2 s} \tag{3.4}$$

with $(a_1, b_1), (a_2, b_2) \in A$ and $0 \leq c_1, c_2 \leq s - 1$.

First consider congruence (3.4) modulo p. We have

$$a \equiv a_1 + a_2 \pmod{p},$$

hence $a_1 + a_2 = a + \delta p$ with $\delta = 0$ or 1. We substitute this into (3.4), substract a and divide by p to obtain

$$c + bs \equiv \delta + c_1 + c_2 + (b_1 + b_2)s \pmod{ps}.$$

We take this modulo s:

$$c \equiv \delta + c_1 + c_2 \pmod{s},$$

consequently $\delta + c_1 + c_2 = c + \eta s$ with $\eta = 0$ or 1. Again substituting back, substracting c and dividing by s we obtain

$$b \equiv \eta + b_1 + b_2 \pmod{p}.$$

So $(a, b) = (a_1, b_1) + (a_2, b_2) + (0, \eta)$ which means that for a, b, η given, we have $\leq g$ possible values of a_1, b_1, a_2, b_2.

Now we are going to find the number of possible values of c_1, c_2 for $a, b, c, \eta, a_1, b_1, a_2, b_2$ given.

Observe that from these data we can calculate $\delta = (a_1 + a_2 - a)/p$. For c_1, c_2 we have the equation $c_1 + c_2 = c - \delta + \eta s$.

If $\eta = 0$, we have $c_1 \leq c$, at most $c + 1$ possibilities.

If $\eta = 1$, we have $c_1 + c_2 \geq c + s - 1$, hence $c - 1 < c_1 \leq s - 1$, which gives at most $s - c$ possibilities.

Hence, if a, b, c, η are given, our estimate is $g(c+1)$ or $g(s-c)$, depending on η. Adding the two estimates we get the claimed bound $g(s+1)$. □

On combining this result with Theorem 3.3.1 we obtain the following result.

Theorem 3.4.2. *For any positive integers k, s, for every sufficiently large prime p, there is a set $A \subseteq \mathbb{Z}_{p^2 s}$ with $(kp - k + 1)s$ elements which is a $\lfloor k^2 + 2k^{3/2} \rfloor (s+1)$-Sidon set.*

Put $q = p^2 s$ and $g = \lfloor k^2 + 2k^{3/2} \rfloor (s+1)$. Thus,

$$\begin{aligned} \frac{\alpha_g(q)}{\sqrt{gq}} \geq \frac{|A|}{\sqrt{gq}} &= \frac{(kp - k + 1)s}{\sqrt{\lfloor k^2 + 2k^{3/2} \rfloor (s+1)p^2 s}} \\ &\geq \frac{(kp - k)s}{\sqrt{(k^2 + 2k^{3/2})(s+1)p^2 s}} \\ &\geq \frac{p - 1}{p\sqrt{(1 + 2/\sqrt{k})(1 + 1/s)}}. \end{aligned}$$

A convenient choice of the parameters is $k = 4s^2$ (so $s = \Theta(g^{1/5})$). Assuming that, we get

$$\frac{\alpha_g(q)}{\sqrt{gq}} \geq \frac{p-1}{p} \cdot \frac{1}{1 + 1/s}.$$

Thus, the Prime Number Theorem says that

$$\frac{\alpha_g}{\sqrt{g}} = \limsup_{q \to \infty} \frac{\alpha_g(q)}{\sqrt{gq}} \geq \limsup_{p \to \infty} \frac{p-1}{p} \cdot \frac{1}{1 + 1/s} = 1 + O(g^{-1/5}),$$

which completes the proof of Theorem 3.1.7.

3.5 Upper bound

We turn now to the proof of Theorem 3.1.5, which says:

$$\lim_{g\to\infty} \liminf_{N\to\infty} \frac{\beta_g(N)}{\sqrt{g}\sqrt{N}} = \lim_{g\to\infty} \limsup_{N\to\infty} \frac{\beta_g(N)}{\sqrt{g}\sqrt{N}} = \sigma.$$

We will prove it in two stages:

Part A.
$$\limsup_{g\to\infty} \limsup_{N\to\infty} \frac{\beta_g(N)}{\sqrt{g}\sqrt{N}} \leq \sigma.$$

Part B.
$$\liminf_{g\to\infty} \liminf_{N\to\infty} \frac{\beta_g(N)}{\sqrt{g}\sqrt{N}} \geq \sigma.$$

For Part A we will use the ideas of Schinzel and Schmidt [29], which give a connection between convolutions and number of representations, between the continuous and the discrete world. For the sake of completeness we rewrite the results and the proofs in a more convenient way for our purposes.

Remember from (3.1) the definition of σ:

$$\sigma = \sup_{f\in\mathcal{F}} \|f\|_1,$$

where $\mathcal{F} = \{f : f \geq 0,\ \mathrm{supp}(f) \subseteq [0,1],\ \|f * f\|_\infty \leq 1\}$.

We will use the next result, which is assertion (ii) of Theorem 1 in [29] (essentially the same result appears in [23] as Corollary 1.5):

Theorem 3.5.1. *Let σ be the constant defined above and $\mathcal{Q}_N = \{Q \in \mathbb{R}_{\geq 0}[x] : Q \not\equiv 0, \deg Q < N\}$. Then*

$$\sup_{Q\in\mathcal{Q}_N} \frac{|Q|_1}{\sqrt{N}\sqrt{|Q^2|_\infty}} \leq \sigma,$$

where $|P|_1$ is the sum and $|P|_\infty$ the maximum of the coefficients of a polynomial P.

Proof. First of all, observe that the definition of σ is equivalent to this one:

$$\sigma = \sup_{f \in \mathcal{F}'} \frac{\|f\|_1}{\sqrt{\|f * f\|_\infty}},$$

where $\mathcal{F}' = \{f : f \geq 0,\ \mathrm{supp}(f) \subseteq [0,1]\}$.

Given a polynomial $Q = a_0 + a_1 x + \ldots + a_{N-1}x^{N-1}$ in $\mathcal{Q}_N$, we define the step function g with support in $[0,1)$ having

$$g(x) = a_i \ \text{ for } \ \frac{i}{N} \leq x < \frac{i+1}{N} \ \text{ for every } \ i = 0, 1, \ldots, N-1.$$

The convolution of this step function with itself is the polygonal function:

$$g*g(x) = \sum_{i=0}^{j} a_i a_{j-i} \left(x - \frac{j}{N}\right) + \sum_{i=0}^{j-1} a_i a_{j-1-i} \left(\frac{j+1}{N} - x\right), x \in \left[\frac{j}{N}, \frac{j+1}{N}\right)$$

for every $j = 0, 1, \ldots, 2N-1$, where we define $a_N = a_{N+1} = \ldots = a_{2N-1} = 0$.

So,

$$\sup_x (g * g)(x) = \frac{1}{N} \sup_{0 \leq j \leq 2N-2} \left(\sum_{i=0}^{j} a_i a_{j-i}\right).$$

Since, obviously, $\int_0^1 g(x)\ dx = \frac{1}{N}\sum_{i=0}^{N-1} a_i$, we have:

$$\frac{|Q|_1}{\sqrt{N}\sqrt{|Q^2|_\infty}} = \frac{\int_0^1 g(x)\ dx}{\sqrt{\sup_x (g*g)(x)}} \leq \sigma.$$

And because we have this for every Q, the theorem is proved. □

Now, given a g-Sidon set $A \subseteq \{0, 1, \ldots, N-1\}$, we define the polynomial $Q_A(x) = \sum_{a \in A} x^a$, so $Q_A^2(x) = \sum_n r(n) x^n$. Then, Theorem 3.5.1 says that

$$\sigma \geq \frac{|Q_A|_1}{\sqrt{|Q_A^2|_\infty}\sqrt{N}} \geq \frac{|A|}{\sqrt{g}\sqrt{N}}.$$

Since this happens for every g-Sidon set in $\{0, 1, \ldots, N-1\}$, we have that

$$\frac{\beta_g(N)}{\sqrt{g}\sqrt{N}} \leq \sigma.$$

This proves Part A of Theorem 3.1.5, which is the easy part.

Remark 3.5.2. In fact, not only Schinzel and Schmidt prove the result above in [29], but they also prove (see Theorem 3.6.1) that

$$\lim_{N\to\infty} \sup_{Q\in\mathcal{Q}_N} \frac{|Q|_1}{\sqrt{N}\sqrt{|Q^2|_\infty}} = \sigma.$$

Newman polynomials are polynomials all of whose coefficients are 0 or 1. In [34], Gang Yu conjectured that for every sequence of Newman polynomials Q_N with $\deg Q_N = N-1$ and $|Q_N|_1 = o(N)$

$$\limsup_{N\to\infty} \frac{|Q_N|_1}{\sqrt{N}\sqrt{|Q_N^2|_\infty}} \leq 1.$$

Greg Martin and Kevin O'Bryant [23] disproved this conjecture, finding a sequence of Newman polynomials with $\deg Q_N = N-1$, $|Q_N|_1 = o(N)$ and

$$\limsup_{N\to\infty} \frac{|Q_N|_1}{\sqrt{N}\sqrt{|Q_N^2|_\infty}} = \frac{2}{\sqrt{\pi}}.$$

In fact, with the probabilistic method it can be proved without much effort that there is a sequence of Newman polynomials, with $\deg Q_N = N-1$ and $|Q_N|_1 = O(N^{1/2}(\log N)^\beta)$ for any given $\beta > 1/2$, such that

$$\limsup_{N\to\infty} \frac{|Q_N|_1}{\sqrt{N}\sqrt{|Q_N^2|_\infty}} = \sigma.$$

Our Theorem 3.1.5 says that given $\varepsilon > 0$, there exists a constant c_ε and a sequence of polynomials, Q_N, with $\deg Q_N = N-1$ and $|Q_N|_1 \leq c_\varepsilon N^{1/2}$

such that

$$\limsup_{N\to\infty} \frac{|Q_N|_1}{\sqrt{N}\sqrt{|Q_N^2|_\infty}} \geq \sigma - \varepsilon.$$

Observe that this growth is close to the best possible, since taking $|Q_N|_1 = o(N^{1/2})$ makes $\frac{|Q_N|_1}{\sqrt{N}\sqrt{|Q_N^2|_\infty}} \to 0$.

3.6 Connecting the discrete and the continuous world

For Part B of the proof of Theorem 3.1.5 we will need another result of Schinzel and Schmidt (assertion (iii) of Theorem 1 in [29]) which we state in a more convenient form for our purposes:

Theorem 3.6.1. *For every $0 < \alpha < 1/2$, for any $0 < \varepsilon < 1$ and for every $n > n(\varepsilon)$, there exist non-negative real numbers $a_0, a_1, \ldots, a_n$ such that*

1. $a_i \leq n^\alpha(1-\varepsilon)$ *for every* $i = 0, 1, \ldots, n$.
2. $\sum_{i=0}^{n} a_i \geq n\sigma(1-\varepsilon)$.
3. $\sum_{0\leq i, m-i\leq n} a_i a_{m-i} \leq n(1+\varepsilon)$ *for every* $m = 0, 1, \ldots, 2n$.

Proof. We start with a real nonnegative function defined in $[0,1]$, g, with $|g * g|_\infty \leq 1$ and $|g|_1$ close to σ, say $|g|_1 \geq \sigma(1-\varepsilon/2)$.

For $r < s$ we have the estimation

$$\begin{aligned}\left(\int_r^s g(x)\ dx\right)^2 &= \int_r^s \int_r^s g(x)g(y)\ dx\ dy \\ &= \int_{r+x}^{s+x} \int_r^s g(x)g(z-x)\ dx\ dz \qquad (3.5)\\ &\leq \int_{2r}^{2s} \int_r^s g(x)g(z-x)\ dx\ dz \leq 2(s-r)\end{aligned}$$

which implies that

$$\int_r^s g(x)\ dx \leq \sqrt{2(s-r)}. \qquad (3.6)$$

Trying to "discretize" our function g, we define for $i = 0, 1, 2, \ldots, n$:

$$a_i = \frac{n}{2L} \int_{(i-L)/n}^{(i+L)/n} g(x)\ dx$$

where $1 \leq L \leq n/2$ is an integer that will be determined later.

Estimation (3.6) proves that

$$a_i \leq \sqrt{n/L} \quad \text{for} \quad i = 0, 1, 2, \ldots, n. \tag{3.7}$$

Now we give a lower bound for the sum $\sum_{i=0}^{n} a_i$:

$$\sum_{i=0}^{n} a_i = \frac{n}{2L} \int_0^1 \nu(x) g(x)\ dx,$$

where

$$\begin{aligned} \nu(x) &= \left| \left\{ i \in [0, n] : \frac{i-L}{n} \leq x \leq \frac{i+L}{n} \right\} \right| \\ &= |\{ i : \max\{0, nx - L\} \leq i \leq \min\{n, nx + L\} \}|. \end{aligned}$$

Taking into account that an interval of length M has $\geq \lfloor M \rfloor$ integers and an interval of length M starting or finishing at an integer has $\lceil M \rceil$ integers, and since $L \in \mathbb{Z}$ and $1 \leq L \leq n/2$, we have

$$\nu(x) \geq \begin{cases} nx + L = 2L - (L - nx) & \text{if } 0 \leq x \leq L/n \\ 2L & \text{if } L/n \leq x \leq 1 - L/n \\ n - nx + L = 2L - (L - n(1-x)) & \text{if } 1 - L/n \leq x \leq 1 \end{cases}$$

and so

$$\begin{aligned} \sum_{i=0}^{n} a_i \quad \geq \quad & n \int_0^1 g(x)\ dx - \frac{n}{2L} \int_0^{L/n} (L - nx) g(x)\ dx \\ & - \frac{n}{2L} \int_{1-L/n}^{1} (L - n(1-x)) g(x)\ dx. \end{aligned}$$

Now, using the fact that $|g|_1 \geq \sigma(1-\varepsilon/2)$ and estimation (3.6),

$$\sum_{i=0}^{n} a_i \geq n\sigma(1-\varepsilon/2) - \sqrt{2nL}. \tag{3.8}$$

Also, for every $m \leq 2n$ we give an upper bound for $\sum_{0\leq i,m-i\leq n} a_i a_{m-i}$.

First we write:

$$\sum_{0\leq i,m-i\leq n} a_i a_{m-i} = \Big(\frac{n}{2L}\Big)^2 \sum_{0\leq i,m-i\leq n} \int_{(m-i-L)/n}^{(m-i+L)/n} \int_{(i-L)/n}^{(i+L)/n} g(x)g(y)\ dx\ dy.$$

Now, as in (3.5), we set $z = x + y$ and we consider the set:

$$S_i = \left\{(x,z) : \frac{i-L}{n} \leq x \leq \frac{i+L}{n} \ \text{ and } \ \frac{m-i-L}{n} \leq z-x \leq \frac{m-i+L}{n}\right\}.$$

Then,

$$\sum_{0\leq i,m-i\leq n} a_i a_{m-i} = \Big(\frac{n}{2L}\Big)^2 \sum_{0\leq i,m-i\leq n} \int\int_{S_i} g(x)g(z-x)\ dx\ dz$$

and, defining $\mu(x,z) = |\{\max\{0,m-n\} \leq i \leq \min\{m,n\} : i-L \leq nx \leq i+L \ \text{ and } \ m-i-L \leq n(z-x) \leq m-i+L\}|$,

$$\sum_{0\leq i,m-i\leq n} a_i a_{m-i} = \Big(\frac{n}{2L}\Big)^2 \int\int \mu(x,z) g(x)g(z-x)\ dx\ dz.$$

If we write $h = i - nx$ then we are imposing $-L \leq h \leq L$ and $m - L - nz \leq h \leq m + L - nz$, so

$$-L + \max\{0, m-nz\} \leq h \leq L + \min\{0, m-nz\},$$

and $\mu(x,z) \leq \lambda(z)$, which is the number of h's in this interval (it could be empty), and this number is clearly $\leq 2L+1$. Also, for each fixed h, z moves

in an interval of length $2L/n$.

This means (remember that $|g * g|_\infty \leq 1$)

$$\begin{aligned}\sum_{0\leq i,m-i\leq n} a_i a_{m-i} &\leq \left(\frac{n}{2L}\right)^2 \int \lambda(z) \int g(x)g(z-x)\ dx\ dz \\ &\leq \left(\frac{n}{2L}\right)^2 \int \lambda(z)\ dz \\ &\leq \left(\frac{n}{2L}\right)^2 \frac{2L(2L+1)}{n}\end{aligned}$$

so the sum

$$\sum_{0\leq i,m-i\leq n} a_i a_{m-i} \leq n\left(1+\frac{1}{2L}\right). \tag{3.9}$$

Finally, looking at (3.7), (3.8) and (3.9), and choosing the integer $L = \lceil n^{1-2\alpha}/(1-\varepsilon)^2 \rceil$ with $0 < \alpha < 1/2$, for sufficiently large n we will have:

$$a_i \leq n^\alpha(1-\varepsilon),\ \ \sum_{i=0}^{n} a_i \geq n\sigma(1-\varepsilon)\ \ \text{and}\ \ \sum_{0\leq i,m-i\leq n} a_i a_{m-i} \leq n(1+\varepsilon).$$

□

Remark 3.6.2. Now, we will construct random sets. We want to use the numbers obtained in Theorem 3.6.1 to define probabilities, p_i, and it will be convenient to know the sum of the p_i's. This is the motivation for defining

$$p_i = a_i \cdot \frac{\sigma n^{1-\alpha}}{\sum_{i=0}^{n} a_i} \quad \text{for} \quad i = 0, 1, \ldots, n.$$

Now we fix $\alpha = 1/3$, although any $\alpha \in (0, 1/2)$ would work. Then we have $p_i = a_i \cdot \dfrac{\sigma n^{2/3}}{\sum_{i=0}^{n} a_i}$, so for any $0 < \varepsilon < 1$ and for every $n > n(\varepsilon)$, we have $p_0, p_1, \ldots, p_n$ such that:

$$p_i \leq 1\ ,\ \ \sum_{i=0}^{n} p_i = \sigma n^{2/3}\ \ \text{and}\ \ \sum_{0\leq i,m-i\leq n} p_i p_{m-i} \leq n^{1/3}\frac{1+\varepsilon}{(1-\varepsilon)^2}.$$

In order to prove that the number of elements and the number of representations in our probabilistic sets are what we expect with high probability, we'll use Chernoff's inequality (see Corollary 1.9 in [32]).

Proposition 3.6.3. ***(Chernoff's inequality)*** *Let $X = t_1 + \cdots + t_n$ where the t_i are independent Boolean random variables. Then for any $\delta > 0$*

$$\mathbb{P}(|X - \mathbb{E}(X)| \geq \delta \mathbb{E}(X)) \leq 2e^{-\min(\delta^2/4, \delta/2)\mathbb{E}(X)}. \tag{3.10}$$

Then, we have the next two lemmas which also appear in [11]:

Lemma 3.6.4. *We consider the probability space of all the subsets $A \subseteq \{0, 1, \ldots, n\}$ defined by $\mathbb{P}(i \in A) = p_i$. With the p_i's defined above, given $0 < \varepsilon < 1$, there exists $n_0(\varepsilon)$ such that, for all $n \geq n_0$,*

$$\mathbb{P}(|A| \geq \sigma n^{2/3}(1 - \varepsilon)) > 0.9.$$

Proof. Since $|A|$ is a sum of independent Boolean variables and $\mathbb{E}(|A|) = \sum_{i=0}^{n} p_i = \sigma n^{2/3}$, we can apply Proposition 3.6.3 to deduce that for large enough n

$$\mathbb{P}(|A| < \sigma n^{2/3}(1 - \varepsilon)) \leq 2e^{-\sigma n^{2/3}\varepsilon^2/4} < 0.1.$$

□

Lemma 3.6.5. *We consider the probability space of all the subsets $A \subseteq \{0, 1, \ldots, n\}$ defined by $\mathbb{P}(i \in A) = p_i$. Again for the p_i's defined above, given $0 < \varepsilon < 1$, there exists $n_1(\varepsilon)$ such that, for all $n \geq n_1$,*

$$r(m) \leq n^{1/3} \left(\frac{1 + \varepsilon}{1 - \varepsilon}\right)^3 \text{ for all } m = 0, 1, \ldots, 2n$$

with probability > 0.9.

Proof. Since $r(m) = \sum_{0 \leq i, m-i \leq n} \mathbb{I}(i \in A)\mathbb{I}(m - i \in A)$ is a sum of Boolean

variables which are not independent, it is convenient to consider

$$r'(m)/2 = \sum_{\substack{0\leq i,m-i\leq n\\ i<m/2}} \mathbb{I}(i\in A)\mathbb{I}(m-i\in A)$$

leaving in mind that $r(m) = r'(m) + \mathbb{I}(m/2 \in A)$.

From the independence of the indicator functions, and following the notation introduced in Definition 3.1.1, the expected value of $r'(m)/2$ is

$$\begin{aligned}\mu_m &= \mathbb{E}(r'(m)/2) = \sum_{\substack{0\leq i,m-i\leq n\\ i<m/2}} \mathbb{E}(\mathbb{I}(i\in A)\mathbb{I}(m-i\in A))\\ &= \sum_{\substack{0\leq i,m-i\leq n\\ i<m/2}} p_i p_{m-i} \leq \frac{n^{1/3}}{2}\cdot\frac{1+\varepsilon}{(1-\varepsilon)^2},\end{aligned}$$

for every $m = 0, 1, \ldots, 2n$, for n large enough.

If $\mu_m = 0$ then $\mathbb{P}(r'(m)/2 > 0) = 0$, so we can consider the next two cases:

- If $\frac{1}{3}\cdot\frac{n^{1/3}(1+\varepsilon)}{2(1-\varepsilon)^2} \leq \mu_m$ then

  $$\mathbb{P}\left(r'(m)/2 \geq \frac{n^{1/3}}{2}\left(\frac{1+\varepsilon}{1-\varepsilon}\right)^2\right) \leq \mathbb{P}(r'(m)/2 \geq \mu_m(1+\varepsilon))$$

  and we can apply Proposition 3.6.3 (observe that $\varepsilon < 2$ and then $\varepsilon^2/4 \leq \varepsilon/2$) to have that this is

  $$\begin{aligned}&\leq 2\exp\left(-\frac{\varepsilon^2\mu_m}{4}\right)\\ &\leq 2\exp\left(-\frac{n^{1/3}\varepsilon^2(1+\varepsilon)}{24(1-\varepsilon)^2}\right)\end{aligned}$$

- If $0 < \mu_m < \frac{1}{3}\cdot\frac{n^{1/3}(1+\varepsilon)}{2(1-\varepsilon)^2}$ then we define $\delta = \frac{n^{1/3}}{2\mu_m}\left(\frac{1+\varepsilon}{1-\varepsilon}\right)^2 - 1$ (observe

that $\delta \geq 2$ and then $\delta/2 \leq \delta^2/4$),

$$\mathbb{P}\left(r'(m)/2 \geq \frac{n^{1/3}}{2}\left(\frac{1+\varepsilon}{1-\varepsilon}\right)^2\right) = \mathbb{P}(r'(m)/2 \geq \mu_m(1+\delta))$$

and then we can apply Proposition 3.6.3 to have that this is

$$\begin{aligned}
&\leq 2\exp\left(-\frac{\delta\mu_m}{2}\right) \\
&= 2\exp\left(-\frac{n^{1/3}}{4}\left(\frac{1+\varepsilon}{1-\varepsilon}\right)^2 + \frac{\mu_m}{2}\right) \\
&\leq 2\exp\left(-\frac{n^{1/3}}{4}\left(\frac{1+\varepsilon}{1-\varepsilon}\right)^2 + \frac{n^{1/3}(1+\varepsilon)}{12(1-\varepsilon)^2}\right) \\
&\leq 2\exp\left(-\frac{n^{1/3}}{6}\left(\frac{1+\varepsilon}{1-\varepsilon}\right)^2\right)
\end{aligned}$$

Then,

$$\begin{aligned}
&\mathbb{P}\left(r'(m)/2 \geq \frac{n^{1/3}}{2}\left(\frac{1+\varepsilon}{1-\varepsilon}\right)^2 \text{ for some } m\right) \\
&\leq 4n\left(\exp\left(-\frac{n^{1/3}\varepsilon^2(1+\varepsilon)}{24(1-\varepsilon)^2}\right) + \exp\left(-\frac{n^{1/3}}{6}\left(\frac{1+\varepsilon}{1-\varepsilon}\right)^2\right)\right)
\end{aligned}$$

which is < 0.1 for n large enough.

Remembering that $r(m) = r'(m) + \mathbb{I}(m/2 \in A)$,

$$\mathbb{P}\left(r(m) \geq n^{1/3}\left(\frac{1+\varepsilon}{1-\varepsilon}\right)^2 + \ \mathbb{I}(m/2 \in A) \ \text{ for some } m\right) < 0.1$$

for n large enough, and finally

$$\mathbb{P}\left(r(m) \geq n^{1/3}\left(\frac{1+\varepsilon}{1-\varepsilon}\right)^3 \text{ for some } m\right) < 0.1 \text{ for } n \text{ large enough.}$$

□

Lemmas 3.6.4 and 3.6.5 imply that, given $0 < \varepsilon < 1$, for every $n \geq \max\{n_0, n_1\}$, the probability that our random set A satisfies $|A| \geq \sigma n^{2/3}(1-\varepsilon)$ and $r(m) \leq n^{1/3}\left(\frac{1+\varepsilon}{1-\varepsilon}\right)^3$ for every m is greater than 0.8. In particular, for every $n \geq \max\{n_0, n_1\}$ we have a set $A \subseteq \{0, 1, \ldots, n\}$ satisfying these conditions.

3.7 From residues to integers

In order to prove Part B of Theorem 3.1.5, we will also need the next lemma, which allows us to "paste" copies of a g_2-Sidon set in a cyclic group with a dilation of a g_1-Sidon set in the integers.

Lemma 3.7.1. *Let $A = \{0 = a_1 < \ldots < a_k\}$ be a g_1-Sidon set in $\mathbb{Z}$ and let $C \subseteq [1, q]$ be a g_2-Sidon set $\pmod q$. Then $B = \cup_{i=1}^{k}(C + qa_i)$ is a g_1g_2-Sidon set with $k|C|$ elements in $[1, q(a_k + 1)]$.*

Proof. Suppose we have $g_1g_2 + 1$ representations of an element as the sum of two

$$b_{1,1} + b_{2,1} = b_{1,2} + b_{2,2} = \cdots = b_{1,g_1g_2+1} + b_{2,g_1g_2+1}.$$

Each $b_{i,j} = c_{i,j} + qa_{i,j}$ in a unique way. Now we can look at the equality modulo q to have

$$c_{1,1} + c_{2,1} = c_{1,2} + c_{2,2} = \cdots = c_{1,g_1g_2+1} + c_{2,g_1g_2+1} \pmod q.$$

Since C is a g_2-Sidon set $\pmod q$, by the pigeonhole principle, there are at least $g_1 + 1$ pairs (c_{1,i_1}, c_{2,i_1}), ..., $(c_{1,i_{g_1+1}}, c_{2,i_{g_1+1}})$ such that:

$$c_{1,i_1} = \cdots = c_{1,i_{g_1+1}} \qquad \text{and} \qquad c_{2,i_1} = \cdots = c_{2,i_{g_1+1}}.$$

So the corresponding a_i's satisfy

$$a_{1,i_1} + a_{2,i_1} = \cdots = a_{1,i_{g_1+1}} + a_{2,i_{g_1+1}},$$

and since A is a g_1-Sidon set, there must be an equality

$$a_{1,k} = a_{1,l} \qquad \text{and} \qquad a_{2,k} = a_{2,l}$$

for some $k, l \in \{i_1, \ldots, i_{g_1+1}\}$.

Then, for these k and l we have

$$b_{1,k} = b_{1,l} \qquad \text{and} \qquad b_{2,k} = b_{2,l},$$

which completes the proof. □

With all these weapons, we are ready to finish our proof.

Given $0 < \varepsilon < 1$ we have that:

a) For every large enough g we can define $n = n(g)$ as the least integer such that $g = \left\lfloor n^{1/3} \left(\frac{1+\varepsilon}{1-\varepsilon}\right)^3 \right\rfloor$, and such an n exists because $n^{1/3} \left(\frac{1+\varepsilon}{1-\varepsilon}\right)^3$ grows more slowly than n. Observe that $n(g) \to \infty$ when $g \to \infty$.

   Now, by lemmas 3.6.4 and 3.6.5, there is $g_0 = g_0(\varepsilon)$ such that for every $g_1 \geq g_0$ we can consider $n = n(g_1)$ and we have a g_1-Sidon set $A \subseteq \{0, 1, \ldots, n\}$ such that

$$\frac{|A|}{\sqrt{g_1}\sqrt{n+1}} \geq \sigma \sqrt{\frac{n}{n+1}} \cdot \frac{(1-\varepsilon)^{5/2}}{(1+\varepsilon)^{3/2}}.$$

b) By Theorem 3.4.2, there are $g_2 = g_2(\varepsilon)$, $s = s(\varepsilon)$ and a sequence $q_0 = p_r^2 s$, $q_1 = p_{r+1}^2 s$, $q_2 = p_{r+2}^2 s$, ... (where p_i is the i-th prime and

$r = r(\varepsilon)$) such that for every $i = 0, 1, 2, \ldots$ there is a g_2-Sidon set $A_i \subseteq \mathbb{Z}_{q_i}$ with

$$\frac{|A_i|}{\sqrt{g_2 q_i}} \geq 1 - \varepsilon.$$

So, given $0 < \varepsilon < 1$:

1) For every $g \geq g_0(\varepsilon) g_2(\varepsilon)$ there is a $g_1 = g_1(g)$ such that

$$g_1 g_2 \leq g < (g_1 + 1) g_2,$$

and we have $n = n(g_1)$ with $g_1 = \left\lfloor n^{1/3} \left(\frac{1-\varepsilon}{1+\varepsilon}\right)^3 \right\rfloor$ and a g_1-Sidon set $A \subseteq \{0, 1, \ldots, n\}$ with

$$\frac{|A|}{\sqrt{g_1}\sqrt{n+1}} \geq \sigma \sqrt{\frac{n}{n+1}} \cdot \frac{(1-\varepsilon)^{5/2}}{(1+\varepsilon)^{3/2}}.$$

2) For any $N \geq (n+1) q_0$, there is an $i = i(N)$ such that

$$(n+1) q_i \leq N < (n+1) q_{i+1},$$

and we have a g_2-Sidon set $\pmod{q_i}$, A_i, with

$$\frac{|A_i|}{\sqrt{g_2 q_i}} \geq 1 - \varepsilon.$$

Then, for any g and N large enough, applying Lemma 3.7.1 we can construct a $g_1 g_2$-Sidon set from A and A_i with $|A||A_i|$ elements in $[1, N]$.

So we have that $\beta_g(N) \geq \beta_{g_1 g_2}(N) \geq |A||A_i|$ and then

$$\begin{aligned} \frac{\beta_g(N)}{\sqrt{g}\sqrt{N}} &\geq \frac{\beta_{g_1 g_2}(N)}{\sqrt{(g_1+1) g_2}\sqrt{(n+1) q_{i+1}}} \\ &\geq \frac{|A||A_i|}{\sqrt{g_1 g_2}\sqrt{(n+1) q_i}} \sqrt{\frac{g_1}{g_1+1}} \sqrt{\frac{q_i}{q_{i+1}}} \end{aligned}$$

$$\geq \quad \sigma \frac{(1-\varepsilon)^{7/2}}{(1+\varepsilon)^{3/2}} \sqrt{\frac{n}{n+1}} \sqrt{\frac{g_1}{g_1+1}} \sqrt{\frac{p_{r+i}}{p_{r+i+1}}}.$$

Finally, as a consequence of the Prime Number Theorem, this means that, given $0 < \varepsilon < 1$, for g and N large enough

$$\frac{\beta_g(N)}{\sqrt{g}\sqrt{N}} \geq \sigma \frac{(1-\varepsilon)^{9/2}}{(1+\varepsilon)^{3/2}}$$

i. e.

$$\liminf_{g\to\infty} \liminf_{N\to\infty} \frac{\beta_g(N)}{\sqrt{g}\sqrt{N}} \geq \sigma.$$

Chapter 4

Autoconvolutions

In a sense, we now know less than before.

Imre Z. Ruzsa

The work of this chapter is a joint work with Máté Matolcsi [24]. We thank Imre Z. Ruzsa, Javier Cilleruelo, Mihail Kolountzakis and Boris Bukh for many valuable suggestions and stimulating discussions on the subject.

4.1 Introduction

Consider the set $\mathcal{F}$ of all nonnegative real functions f with integral 1, supported on the interval $[-\frac{1}{4}, \frac{1}{4}]$. What is the minimal possible value for the supremum of the autoconvolution $f * f$? It has repeatedly been conjectured $\pi/2$ ([29], [23]), which was the starting point and motivation for the present work. The problem can also be stated in a probabilistic language. We can regard f as the density function of two identically distributed random variables, X and Y. Then, the density function of $X + Y$ is given by the autoconvolution $f * f$, and we are asking for the infimum of the supremum of the density function of the sum $X + Y$.

Define the autoconvolution of f as

$$f * f(x) = \int f(t) f(x - t)\, dt.$$

We are thus interested in

$$S = \inf_{f \in \mathcal{F}} \|f * f\|_\infty$$

where the infimum is taken over all functions f satisfying the above restrictions.

Observe the relation[21] between S and the constant σ defined in Chapter 3. Remember from (3.1) the definition of σ:

$$\sigma = \sup_{f \in \mathcal{F}} \|f\|_1,$$

where $\mathcal{F} = \{f : f \geq 0,\ \mathrm{supp}(f) \subseteq [0,1],\ \|f * f\|_\infty \leq 1\}$.

As we observed in the proof of Theorem 3.5.1, since for a positive real constant C we have $\|Cf\|_1 = C\|f\|_1$ and $\|Cf * Cf\|_\infty = C^2\|f * f\|_\infty$, the definition of σ is equivalent to this one:

$$\sigma = \sup_{f \in \mathcal{F}'} \frac{\|f\|_1}{\sqrt{\|f * f\|_\infty}},$$

where $\mathcal{F}' = \{f : f \geq 0,\ \mathrm{supp}(f) \subseteq [0,1]\}$ (of course we are considering functions with non zero integral).

In the same way, and since translations are irrelevant to our problem, the definition of our constant S is equivalent to:

$$S = \inf_{g \in \mathcal{G}} \frac{\|g * g\|_\infty}{\|g\|_1^2},$$

where $\mathcal{G} = \{g : g \geq 0,\ \mathrm{supp}(g) \subseteq [0,1/2]\}$ (again our functions have non zero integral).

Since if we define $f(x) = g(x/2)$ we have $\|f\|_1 = 2\|g\|_1$ and $\|f * f\|_\infty = 2\|g * g\|_\infty$, we can write

$$S = 2 \inf_{f \in \mathcal{F}'} \frac{\|f * f\|_\infty}{\|f\|_1^2} = 2 \sup_{f \in \mathcal{F}'} \left(\frac{\|f\|_1^2}{\|f * f\|_\infty} \right)^{-1},$$

where $\mathcal{F}'$ is defined above.

[21] This change of terminology is due to the fact that we will follow the notation in [23] so we can directly borrow their results.

So finally

$$S = \frac{2}{\sigma^2}, \text{ or in other words } \sigma = \sqrt{\frac{2}{S}}. \tag{4.1}$$

The question of finding the value of S (or equivalent formulations of it) has been studied in several papers recently [29, 22, 34, 23], and is motivated by its discrete analogue, the study of the maximal possible cardinality of g-Sidon sets (or $B_2[g]$ sets) in $\{1, \ldots, n\}$. The connection between $B_2[g]$ sets and autoconvolutions is described (besides several additional results) in [22, 11, 9] (see Chapter 3).

Translating Theorem 3.1.5 to our new notation (remember 4.1),

$$\lim_{g\to\infty} \frac{\underline{\beta}_g}{\sqrt{g}} = \lim_{g\to\infty} \frac{\overline{\beta}_g}{\sqrt{g}} = \frac{2}{S},$$

which shows explicitly the relation between g-Sidon sets and the constant S.

We give two contributions to the subject. On the one hand, in Section 4.3 we improve the best known lower bound on S. This is achieved by following the ideas of Yu [34], and Martin & O'Bryant [23], and improving them in two minor aspects. On the other hand, maybe more interestingly, Section 4.4 provides counterexamples to a long-standing natural conjecture of Schinzel and Schmidt [29] concerning the extremal function for such autoconvolutions. In some sense these examples open up the subject considerably: at this point we do not have any natural conjectures for the exact value of S or any extremal functions where this value could be attained. Upon numerical evidence we are inclined to believe that $S \approx 1.5$, unless there exists some hidden "magical" number theoretical construction yielding a much smaller value (the possibility of which is by no means excluded).

In short, we will prove

$$1.2748 \leq S \leq 1.5098 \tag{4.2}$$

which improves the best lower and upper bounds that were known for S. As we announced in Subsection 3.1.1, it also implies the improved bounds

$$1.1509... \leq \lim_{g\to\infty} \frac{\underline{\beta}_g}{\sqrt{g}} = \lim_{g\to\infty} \frac{\overline{\beta}_g}{\sqrt{g}} \leq 1.2525.... \tag{4.3}$$

4.2 Notation

We will use the following notation (mostly borrowed from [23]).

Let $\mathcal{F}$ denote the set of nonnegative real functions f supported on the interval $[-1/4, 1/4]$ such that $\int f(x)\,dx = 1$. We define the autoconvolution of f, $f * f(x) = \int f(t)f(x-t)\,dt$ and its autocorrelation, $f \circ f(x) = \int f(t)f(x+t)\,dt$. We are interested in $S = \inf_{f\in\mathcal{F}} \|f * f\|_\infty$. We remark here that the value of S does not change if one considers nonnegative step functions in $\mathcal{F}$ only. This is proved in Theorem 1 in [29]. Therefore the reader may assume that f is square integrable whenever this is needed.

We will need a parameter $0 < \delta \leq 1/4$ and use the notation $u = 1/2 + \delta$, and $\tilde{g}(\xi) = \frac{1}{u}\int_{\mathbb{R}} g(x)e^{-2\pi i x\xi/u}dx$ for any function g. We will also use Fourier coefficients of period 1, i.e. $\hat{g}(\xi) = \int_{\mathbb{R}} g(x)e^{-2\pi i x\xi}\,dx$ for any function g.

We will need a nonnegative kernel function K supported in $[-\delta, \delta]$ with $\int K = 1$. We will also need that $\tilde{K}(j) \geq 0$ for every integer j. We are quite convinced that the choice of K in [23] is optimal, and we will not change it (see equation (4.8) below).

4.3 An improved lower bound

We will follow the steps of [23] (which, in turn, is based on [34]). We include here all the ingredients for convenience (the proofs can be found in [23]).

Lemma 4.3.1. [Lemmas 3.1, 3.2, 3.3, 3.4 in [23]] *With the notation f, K, δ, u as described above, we have*

$$\int (f * f(x))K(x)\,dx \le \|f * f\|_\infty. \tag{4.4}$$

$$\int (f \circ f(x))K(x)\,dx \le 1 + \sqrt{\|f * f\|_\infty - 1}\sqrt{\|K\|_2^2 - 1}. \tag{4.5}$$

$$\int (f * f(x) + f \circ f(x))K(x)\,dx = \frac{2}{u} + 2u^2 \sum_{j\neq 0} (\Re \tilde{f}(j))^2 \tilde{K}(j). \tag{4.6}$$

Let G be an even, real-valued, u-periodic function that takes positive values on $[-1/4, 1/4]$, and satisfies $\tilde{G}(0) = 0$. Then

$$u^2 \sum_{j\neq 0} (\Re \tilde{f}(j))^2 \tilde{K}(j) \ge \left(\min_{0\le x\le 1/4} G(x)\right)^2 \cdot \left(\sum_{j:\tilde{G}(j)\neq 0} \frac{\tilde{G}(j)^2}{\tilde{K}(j)}\right)^{-1}. \tag{4.7}$$

The paper [23] uses the parameter $\delta = 0.13$ (thus $u = 0.63$), and the kernel function

$$K(x) = \frac{1}{\delta}\beta \circ \beta\left(\frac{x}{\delta}\right) \quad \text{where } \beta(x) = \frac{2/\pi}{\sqrt{1-4x^2}} \quad \left(-\frac{1}{2} < x < \frac{1}{2}\right) \tag{4.8}$$

(note here that $\|K\|_2^2 < 0.5747/\delta$). Finally, in equation (4.7) they use one of Selberg's functions, $G(x) = G_{0.63,22}(x)$ defined in Lemma 2.3 of [23]. Combining the statements of Lemma 4.3.1 above they obtain

$$\begin{aligned} &\|f * f\|_\infty + 1 + \sqrt{\|f * f\|_\infty - 1}\sqrt{\|K\|_2^2 - 1} \ge \\ &\ge \frac{2}{u} + 2\left(\min_{0\le x\le 1/4} G(x)\right)^2 \cdot \left(\sum_{j:\tilde{G}(j)\neq 0} \frac{\tilde{G}(j)^2}{\tilde{K}(j)}\right)^{-1} \end{aligned} \tag{4.9}$$

and substituting the values and estimates they have for u, $\tilde{G}(j)$, $\tilde{K}(j)$, $\min_{0\le x\le 1/4} G(x)$ and $\|K\|_2^2$ the bound $\|f * f\|_\infty \ge 1.262$ follows.

Our improvement of the lower bound on $\|f * f\|_\infty$ comes in two steps. First, we find a better kernel function G in equation (4.9). This is indeed plausible because Selberg's functions $G_{u,n}$ do not correspond to the specific choice of K in [23] in any way, therefore we can expect an improvement by choosing G so as to minimize the sum $\sum_{j:\tilde{G}(j)\neq 0} \frac{\tilde{G}(j)^2}{\tilde{K}(j)}$, while keeping $\min_{0\leq x\leq 1/4} G(x) \geq 1$.

Next, we observe that if $\|f*f\|_\infty$ is small then the first Fourier coefficient of f must also be small in absolute value, and we use this information to get a slight further improvement. We will also indicate how the method could yield further improvements.

Theorem 4.3.2. *If $f : [\frac{-1}{4}, \frac{1}{4}] \to \mathbb{R}_+$ is a nonnegative function with $\int f = 1$, then $\|f * f\|_\infty \geq 1.2748$.*

Proof. Let $K(x)$ be defined by (4.8). As in [23] we make use of the facts that $\|K\|_2^2 < 0.5747/\delta$, and $\tilde{K}(j) = \frac{1}{u}|J_0(\pi\delta j/u)|^2$ where J_0 is the Bessel J-function of order 0.

As described above, the main improvement comes from finding a better kernel function G in equation (4.9). Indeed, if we set

$$G(x) = \sum_{j=1}^{n} a_j \cos(2\pi j x/u),$$

then $\tilde{G}(j) = \frac{a_{|j|}}{2}$ for $-n \leq j \leq n$ ($j \neq 0$), and thus equation (4.9) takes the form

$$\begin{aligned} &\|f * f\|_\infty + 1 + \sqrt{\|f * f\|_\infty - 1}\sqrt{0.5747/\delta - 1} \geq \\ &\geq \frac{2}{u} + \frac{4}{u}\left(\min_{0\leq x\leq 1/4} G(x)\right)^2 \cdot \left(\sum_{j=1}^{n} \frac{a_j^2}{|J_0(\pi\delta j/u)|^2}\right)^{-1}. \end{aligned} \tag{4.10}$$

For brevity of notation let us introduce the "gain-parameter"

$$a = \frac{4}{u}\left(\min_{0\le x\le 1/4} G(x)\right)^2 \left(\sum_{j=1}^{n} \frac{a_j^2}{|J_0(\pi\delta j/u)|^2}\right)^{-1}.$$

We note for the record that $a \approx 0.0342$ for the choices $\delta = 0.13$ and $G(x) = G_{0.63,22}(x)$ in [23]. For any fixed δ we are therefore led to the problem of maximizing a (while we may as well assume that $\min_{0\le x\le 1/4} G(x) \ge 1$, as G can be multiplied by any constant without changing the gain a). This problem seems hopeless to solve analytically, but one can perform a numerical search using e.g. the "Mathematica 6" software. Having done so, we obtained that for $\delta = 0.138$ and $n = 119$ there exists a function $G(x)$ with the desired properties such that $a > 0.0713$. The coefficients a_j of $G(x)$ are given in Appendix A. Therefore, using this function $G(x)$ and $\delta = 0.138$ in equation (4.10) we obtain $S \ge 1.2743$.

Remark. One can wonder how much further improvement could be possible by choosing the optimal δ and the optimal $G(x)$ corresponding to it. The answer is that there is *very little* room left for further improvement, the theoretical limit of the argument being somewhere around 1.276. To see this, let $f_s(x) = \frac{1}{2}(f(x) + f(-x))$ denote the symmetrization of f, let $\beta_\delta(x) = \frac{1}{\delta}\beta(\frac{x}{\delta})$ (where $\beta(x)$ is defined in (4.8)) and reformulate equation (4.6) as follows:

$$\begin{aligned}\int (f * f(x) + f \circ f(x))K(x)\,dx &= 2\int (f_s * \beta_\delta(x))^2 dx \\ &= 2\|f_s * \beta_\delta\|_2^2. \qquad (4.11)\end{aligned}$$

This equality is easy to see using Parseval and the fact that $\tilde{K}(j) = u(\tilde{\beta}_\delta(j))^2$. Now, with $\beta_\delta(x)$ being given, the best lower bound we can possibly hope to obtain for the right hand side is $\inf_{f_s} \|f_s * \beta_\delta\|_2^2$, where the infimum is taken over all nonnegative, symmetric functions f_s with integral 1. To calculate this infimum, one can discretize the problem, i. e. approximate

$\beta_\delta(x)$ and $f_s(x)$ by step functions, the heights of the steps of f_s being parameters. Then one can minimize the arising multivariate quadratic polynomial by computer. Finally, we can use equations (4.4), (4.5) and (4.11) to obtain a lower bound for $\|f*f\|_\infty$. We have done this[22] for several values of δ and it seems that best lower bound is achieved for $\delta \approx 0.14$ where we obtain $\|f*f\|_\infty \geq 1.276$. We remark that all this could be done rigorously, but one needs to control the error arising from the discretization, and the sheer documentation of it is simply not worth the effort, in view of the minimal gain.

We can further improve the obtained result a little bit by exploiting some information on the Fourier coefficients of f. For this we need two easy lemmas.

Lemma 4.3.3. *Using the notation $z_1 = |\hat{f}(1)|$ and $k_1 = \hat{K}(1) = \hat{K}(-1)$, where K is defined by equation* (4.8)*, we have*

$$\begin{aligned} &\int (f \circ f(x))K(x)dx \leq \\ &\leq 1 + 2z_1^2 k_1 + \sqrt{\|f*f\|_\infty - 1 - 2z_1^4}\sqrt{\|K\|_2^2 - 1 - 2k_1^2}. \end{aligned} \tag{4.12}$$

Proof. This is an obvious modification of Lemma 3.2 in [23]. Namely,

$$\begin{aligned} \int (f \circ f(x))K(x)dx &= \sum_{j\in\mathbb{Z}} (\widehat{f \circ f}(j))\hat{K}(j) \\ &= 1 + 2z_1^2 k_1 + \sum_{j\neq 0,\pm 1} |\hat{f}(j)|^2 \hat{K}(j) \\ &\leq 1 + 2z_1^2 k_1 + \sqrt{\sum_{j\neq 0,\pm 1} |\hat{f}(j)|^4}\sqrt{\sum_{j\neq 0,\pm 1} \hat{K}(j)^2} \end{aligned}$$

$$\begin{aligned} &= 1 + 2z_1^2 k_1 + \sqrt{\|f*f\|_2^2 - 1 - 2z_1^4}\sqrt{\|K\|_2^2 - 1 - 2k_1^2} \\ &\leq 1 + 2z_1^2 k_1 + \sqrt{\|f*f\|_\infty - 1 - 2z_1^4}\sqrt{\|K\|_2^2 - 1 - 2k_1^2}. \end{aligned}$$

□

[22] We are grateful to Mihail Kolountzakis for pointing out that this minimization problem can indeed be solved numerically due to convexity arguments.

The next observation is that z_1 must be quite small if $\|f * f\|_\infty$ is small. This is established by an application of the following general fact (the discrete version of which is contained in [15]).

Lemma 4.3.4. *If h is a nonnegative function with $\int h = 1$, supported on the interval $[-\frac{1}{2}, \frac{1}{2}]$ and bounded above by M, then $|\hat{h}(1)| \leq \frac{M}{\pi} \sin \frac{\pi}{M}$.*

Proof. Observe first that

$$\hat{h}(1) = \int_{\mathbb{R}} h(x) e^{-2\pi i x}\, dx = e^{-2\pi i t} \int_{\mathbb{R}} h(x+t) e^{-2\pi i x}\, dx$$

and with a suitable choice of t, the last integral, $\int_{\mathbb{R}} h(x+t)e^{-2\pi i x}\, dx$, becomes real and nonnegative. Taking absolute values we get

$$|\hat{h}(1)| = \int_{\mathbb{R}} h(x+t)\cos(2\pi x) dx.$$

The lemma becomes obvious now, because in order to maximize this integral, $h(x+t)$ needs to be concentrated on the largest values of the cosine function, so

$$|\hat{h}(1)| \leq \int_{-\frac{1}{2M}}^{\frac{1}{2M}} M\cos(2\pi x)\, dx = \frac{M}{\pi} \sin \frac{\pi}{M}.$$

□

It is now easy to conclude the proof of Theorem 4.3.2. Assume $\|f*f\|_\infty < 1.2748$. By Lemma 4.3.4 we conclude that

$$|\hat{f}(1)| = \sqrt{|\widehat{f*f}(1)|} \leq \sqrt{\frac{1.2748}{\pi} \sin \frac{\pi}{1.2748}} < 0.50426.$$

However, using Lemma 4.3.3 instead of equation (4.5) we can replace equation (4.10) by

$$\begin{aligned} \frac{2}{u} + a &\leq \|f*f\|_\infty + 1 + 2z_1^2 k_1 + \\ &+ \sqrt{\|f*f\|_\infty - 1 - 2z_1^4}\sqrt{0.5747/\delta - 1 - 2k_1^2} \end{aligned} \tag{4.13}$$

Substituting $\delta = 0.138$, $k_1 = |J_0(\pi\delta)|^2$ and $a = 0.0713$ we obtain a lower bound on $\|f * f\|_\infty$ as a function of z_1. This function $l(z_1)$ is monotonically decreasing in the interval $[0, 0.50426]$ therefore the smallest possible value for $\|f * f\|_\infty$ is attained when we put $z_1 = 0.50426$. In that case we get $\|f * f\|_\infty = 1.27481$, which concludes the proof of the theorem. □

Remark. In principle, the argument above could be improved in several ways.

First, Lemma 4.3.4 does not exploit the fact that $h(x)$ is an autoconvolution. It is possible that a much better upper bound on $|\hat{h}(1)|$ can be given in terms of M if we exploit that $h = f * f$.

Second, for any value of $\delta \leq 1/4$ and any suitable kernel functions K and G we obtain a lower bound, $l(z_1)$, for $\|f * f\|_\infty$ as a function of z_1. A bound $\|f * f\|_\infty \geq s_0$ will follow if z_1 does not fall into the "forbidden set" $F = \{x : l(x) < s_0\}$. In the argument above we put $s_0 = 1.2748$ and, with our specific choices of δ, K and G, the forbidden set was the interval $F = (0.504433, 0.529849)$, and we could prove that z_1 must be outside this set. However, when altering the choices of δ, K and G the forbidden set F also changes. In principle it could be possible that two such sets F_1 and F_2 are disjoint, in which case the bound $\|f * f\|_\infty \geq s_0$ follows automatically.

Third, it is possible to pull out further Fourier coefficients from the Parseval sum in Lemma 4.3.3, and analyze the arising functions $l(z_1, z_2, \dots)$.

4.4 Counterexamples

Some papers in the literature conjectured that $S = \pi/2$, with the extremal function being

$$f_0(x) = \frac{1}{\sqrt{2x + 1/2}}, \ x \in \left(-\frac{1}{4}, \frac{1}{4}\right).$$

Note that $\|f_0 * f_0\|_\infty = \pi/2 = 1.57079\ldots$ In particular, the last remark of [29] seems to be the first instance where $\pi/2$ is suggested as the extremal value, while the recent paper [23] includes this conjecture explicitly as Conjecture 5.1. In this section we disprove this conjecture by means of specific examples. The down side of such examples, however, is that we do not arrive at any reasonable new conjecture for the true value of S or the extremal function where it is attained.

The results of this section are produced by computer search and we do not consider them deep mathematical achievements. However, we believe that they are important contributions to the subject, mostly because they can save considerable time and effort in the future to be devoted to the proof of a natural conjecture which is in fact false. We also emphasize here that although we disprove the conjectures made in [29] and in [23], this does not reduce the value of the main results of those papers in any way.

The counterexamples are produced by a computer search. This is most conveniently carried out in the discretized version of the problem. That is, we take an integer n and consider only nonnegative step functions which take constant values a_j on the intervals $[-\frac{1}{4}+\frac{j}{2n}, -\frac{1}{4}+\frac{j+1}{2n})$ for $j = 0, 1, \ldots, n-1$. This is equivalent to considering all the nonzero polynomials $P(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ with nonnegative coefficients such that $\sum_{j=0}^{n-1} a_j = \sqrt{2n}$ and their squares $P^2(x) = b_0 + b_1x + \cdots + b_{2n-2}x^{2n-2}$, and asking for the infimum of the maximum of the b_j's. Schinzel and Schmidt proved [29] that this value is $\geq S$ and its limit when $n \to \infty$ is S.

Note 4.4.1. As we did in the continuous version, we can also give an equivalent definition of S in the discrete version. We can consider the set $\mathcal{P}$ of all nonzero polynomials of degree $\leq n-1$ with nonnegative real coefficients $P(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ and their squares $P^2(x) = b_0 + b_1x + \cdots + b_{2n-2}x^{2n-2}$ and ask for the value of

$$2n \inf_{P \in \mathcal{P}} \frac{\max_j b_j}{\left(\sum_{j=0}^{n-1} a_j\right)^2}, \tag{4.14}$$

and we will obtain the same value S as before.

Although our examples will be "normalized" in order to fit the first definitions (i.e. all integrals will be normalized to 1, and all sums will be normalized to $\sqrt{2n}$), most of the computations we have been carried out using these other ones (which are more convenient and closer to the ones given by Schinzel and Schmidt). This note also justifies the fact that it is not a problem if we have an integral which is not exactly equal to 1 or a sum of coefficients in a polynomial which is not exactly equal to $\sqrt{2n}$ because of small numerical errors.

While we can only search for *local* minima numerically, using the "Mathematica 6" software we have been able to find examples of step functions with $\|f * f\|_\infty < 1.522$, much lower than $\pi/2$. Subsequently, better examples were produced with the LOQO solver (Student version for Linux and on the NEOS server[23]), reaching the value $\|f * f\|_\infty = 1.51237....$ The best example we are currently aware of has been produced by an iterative algorithm designed by Mihail Kolountzakis and Máté Matolcsi. The idea is as follows: take any step function $f = (a_0, a_1, \ldots, a_{n-1})$ as a starting point, normalized so that $\sum a_j = \sqrt{2n}$. By means of linear programming it is easy (and quick) to find the step function $g_0 = (b_0, b_1, \ldots, b_{n-1})$ which maximizes $\sum b_j$ while keeping $\|f * g_0\|_\infty \leq \|f * f\|_\infty$ (obviously, $\sum b_j \geq \sqrt{2n}$ because the choice $g_0 = f$ is legitimate). We then re-normalize g_0 as $g = \frac{\sqrt{2n} g_0}{\sum b_j}$. Then $\|f * g\|_\infty \leq \|f * f\|_\infty$ by construction. If the inequality is strict then it is easy to see that for small $t > 0$ the function $h = (1-t)f + tg$ will be better than our original f, i. e. $\|h * h\|_\infty \leq \|f * f\|_\infty$. And we iterate this procedure until a fix-point function is reached.

The best example produced by this method is included in Appendix A, achieving the value $\|f * f\|_\infty = 1.50972....$ Figure 4.1 shows a plot of the autoconvolution of this function.

[23]We are grateful to Imre Barany and Robert J. Vanderbei who helped us with a code for LOQO.

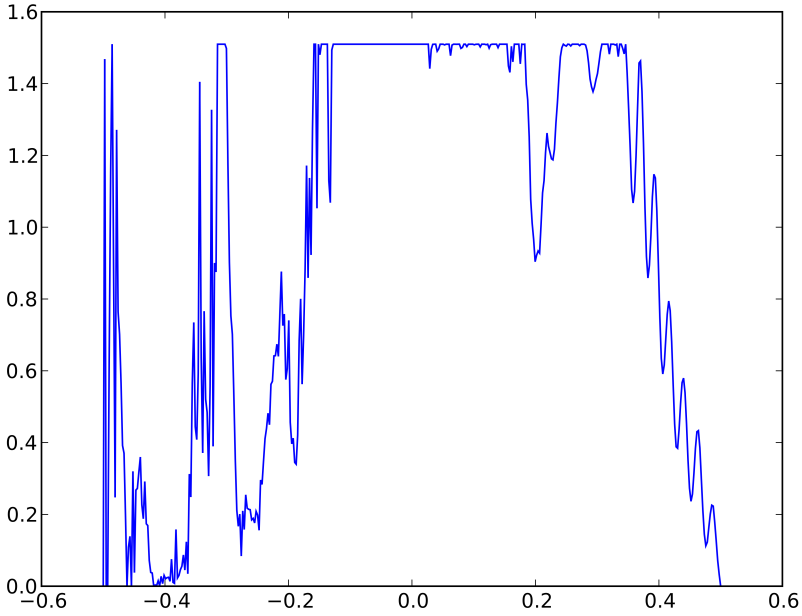

Figure 4.1: The autoconvolution of the best step function we are aware of, giving $\|f * f\|_\infty = 1.50972...$

Interestingly, it seems that the smallest value of n for which a counter-example exists is as low as $n = 10$, giving the value 1.56618... We include the coefficients of one of these polynomials here, as it is fairly easy to check even by hand:

```
0.41241661  0.45380115  0.51373388  0.6162143  0.90077119
0.14003277  0.16228556  0.19989487  0.2837527  0.78923292
```

The down side of such examples is that it seems virtually impossible to guess what the extremal function might be. We have looked at the plot of many step functions f with integral 1 and $\|f * f\|_\infty < 1.52$ and several different patterns seem to arise, none of which corresponds to an easily identifiable function. Looking at one particular pattern we have been able

to produce an analytic formula for a function f which gives a value for $\|f * f\|_\infty \approx 1.52799$, comfortably smaller than $\pi/2$ but which is somewhat far from the minimal value we have achieved with step functions. This function f is given as:

$$f(x) = \begin{cases} \dfrac{1.392887}{(0.00195 - 2x)^{1/3}} & \text{if } \ x \in (-1/4, 0) \\ \\ \dfrac{0.338537}{(0.500166 - 2x)^{0.65}} & \text{if } \ x \in (0, 1/4) \end{cases} \tag{4.15}$$

Figure 4.2 shows a plot of the autoconvolution of this function.

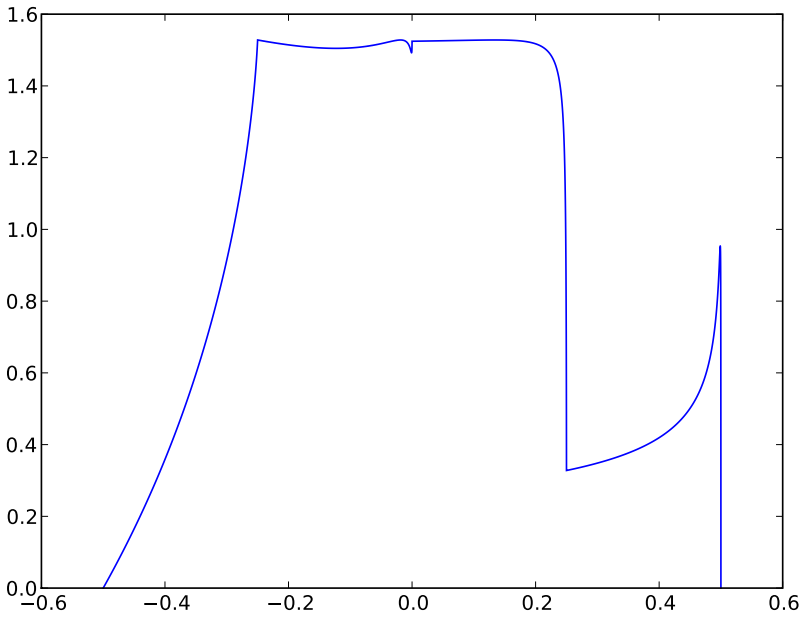

Figure 4.2: The autoconvolution of the function given by equation (4.15), giving $\|f * f\|_\infty \approx 1.52799$.

The paper [23] also states in Conjecture 2 that an inequality of the form

$$\|f * f\|_2^2 \leq c\|f * f\|_\infty \|f * f\|_1 \tag{4.16}$$

should be true with the constant $c = \frac{\log 16}{\pi}$, and once again the function f_0 above producing the extremal case. While we tend to believe that such an inequality is indeed true with some constant $c < 1$, we have been able to disprove this conjecture too, and find examples where $c > \frac{\log 16}{\pi}$. We have not made extensive efforts to maximize the value of c in our numerical search. In Appendix A we include one example of a step function with $n = 20$ where $c = 0.88922... > \frac{\log 16}{\pi} = 0.88254...$

We make a last remark here that could be of interest. It is somewhat natural to believe that the minimal possible value of $\|f*f\|_\infty$ does not change if we allow f to take negative values (but keeping $\int f = 1$). However, this does not seem to be the case. We have found examples of step functions f for which $\|f * f\|_\infty = 1.45810...$, much lower than the best value ($\|f * f\|_\infty = 1.50972...$) we have for nonnegative functions f. This example is also included in Appendix A.

Bibliography

[1] N. Alon, J. H. Spencer, *The Probabilistic Method*. Wiley-Interscience (2000).

[2] R. C. Bose, *An afine analogue of Singer's theorem*. J. Indian Math. Soc., vol. 6, 1-15 (1942).

[3] Boris Bukh, *Sums of dilates*. Combinatorics, Probability and Computing, vol. 17, 627-639 (2008).

[4] J. Cilleruelo, *An upper bound for $B_2[2]$ sequences*. J. Combin. Theory, Ser. A, vol. 89, n° 1, 141-144 (2000).

[5] J. Cilleruelo, *Probabilistic constructions of $B_2[g]$ sequences*. To appear in Acta Mathematica Sinica (2009).

[6] J. Cilleruelo, *Sidon sets in $\mathbb{N}^d$*. Preprint (2009).

[7] J. Cilleruelo, S. Z. Kiss, I. Z. Ruzsa, C. Vinuesa, *Generalization of a theorem of Erdős and Rényi on Sidon Sequences*. Preprint (2009).

[8] J. Cilleruelo, I. Z. Ruzsa and C. Trujillo, *Upper and lower bounds for finite $B_h[g]$ sequences*. J. Number Theory 97, 26-34 (2002).

[9] J. Cilleruelo, I. Z. Ruzsa, C. Vinuesa, *Generalized Sidon Sets*. arXiv:0909.5024v1 (2009).

[10] J. Cilleruelo, M. Silva, C. Vinuesa, *A Sumset Problem*. To appear in Journal of Combinatorics and Number Theory (2009).

[11] J. Cilleruelo, C. Vinuesa, *$B_2[g]$ sets and a conjecture of Schinzel and Schmidt*. Combinatorics, Probability and Computing, vol. 17, n° 6, 741-747 (2008).

[12] P. Erdős and A. Rényi, *Additive properties of random sequences of positive integers*. Acta Arithmetica 6, 85-110 (1960).

[13] P. Erdős and P. Tetali, *Representations of Integers as the Sum of k terms*. Random Structures and Algorithms, vol. 1, n° 3 (1990).

[14] P. Erdős and P. Turán, *On a problem of Sidon in additive number theory, and on some related problems*. J. London Math. Soc. 16, 212-215 (1941).

[15] B. Green, *The number of squares and $B_h[g]$ sets*. Acta Arith. 100, n° 4, 365-390 (2001).

[16] L. Habsieger and A. Plagne, *Ensembles $B_2[2]$: l'étau se resserre*. Integers 2, Paper A2, 20 pp., electronic (2002).

[17] H. Halberstam and K. F. Roth, *Sequences*. Springer - Verlag, New York (1983).

[18] M. Kolountzakis, *The Density of Sets and the Minimum of Dense Cosine Sums*. J. Number Theory 56, 1, 4-11 (1996).

[19] B. Lindström, *An inequality for B_2-sequences*. J. Combinatorial Theory 6, 211-212 (1969).

[20] B. Lindström, *$B_h[g]$-sequences from B_h-sequences*. Proc. Amer. Math. Soc. 128, 657-659 (2000).

[21] G. Martin, K. O'Bryant, *Constructions of Generalized Sidon Sets*. Journal of Combinatorial Theory, Series A, vol. 113, Issue 4, 591-607 (2006).

[22] G. Martin, K. O'Bryant, *The Symmetric Subset Problem in Continuous Ramsey Theory*. Experiment. Math., vol. 16, n° 2, 145-166 (2007).

[23] G. Martin, K. O'Bryant, *The supremum of autoconvolutions, with applications to additive number theory*. arXiv:0807.5121v2. To appear in IJM (2009).

[24] M. Matolcsi, C. Vinuesa, *Improved bounds on the supremum of autoconvolutions*. arXiv:0907.1379v2 (2009).

[25] Melvin B. Nathanson, *Inverse problems for linear forms over finite sets of integers*. arXiv:0708.2304 (2007).

[26] A. Plagne, *A new upper bound for $B_2[2]$ sets*. J. Combin. Theory, Ser. A 93, 378-384 (2001).

[27] A. Plagne, *Recent progress on finite $B_h[g]$ sets*. Proceedings of the Thirty-Second Southeastern International Conference on Combinatorics, Graph Theory and Computing (Baton Rouge, LA, 2001), vol. 153, 49-64 (2001).

[28] I. Z. Ruzsa, *Solving a linear equation in a set of integers I*. Acta Arithmetica 65, 259-282 (1993).

[29] A. Schinzel, W. M. Schmidt, *Comparison of L^1- and $L^\infty-$ norms of squares of polynomials*. Acta Arithmetica 104, n° 3, 283-296 (2002).

[30] S. Sidon, *Ein Satz über trigonometrische Polynome und seine Anwendungen in der Theorie der Fourier-Reihen*. Math. Annalen 106, 536-539 (1932).

[31] J. Singer, *A theorem in finite projective geometry and some applications to number theory*. Trans. Amer. Math. Soc. 43 , 377-385 (1938).

[32] T. Tao, V. H. Vu, *Additive Combinatorics*. Cambridge University Press (2006).

[33] V. H. Vu, *On a refinement of Waring's problem*. Duke Math. J., vol. 105, n° 1 107-134 (2000).

[34] G. Yu, *An upper bound for $B_2[g]$ sets*. J. Number Theory 122, n° 1, 211-220 (2007).

Appendix A

Numbers

Suppose aliens invade the Earth and threaten to obliterate it in a year's time unless human beings can find the Ramsey number for red five and blue five. We could marshal the world's best minds and fastest computers, and within a year we could probably calculate the value. If the aliens demanded the Ramsey number for red six and blue six, however, we would have no choice but to launch a preemptive attack.

Paul Erdös

Here we list the numerical values corresponding to the results of Chapter 4.

For $\delta = 0.138$ (and thus $u = 0.638$) we define the kernel function $G(x)$ used in Theorem 4.3.2 as $G(x) = \sum_{j=1}^{119} a_j \cos(2\pi jx/u)$, with the coefficients a_j given by the following list:

```
 2.16620392e+00  -1.87775750e+00   1.05828868e+00  -7.29790538e-01
 4.28008515e-01   2.17832838e-01  -2.70415201e-01   2.72834790e-02
-1.91721888e-01   5.51862060e-02   3.21662512e-01  -1.64478392e-01
 3.95478603e-02  -2.05402785e-01  -1.33758316e-02   2.31873221e-01
-4.37967118e-02   6.12456374e-02  -1.57361919e-01  -7.78036253e-02
 1.38714392e-01  -1.45201483e-04   9.16539824e-02  -8.34020840e-02
-1.01919986e-01   5.94915025e-02  -1.19336618e-02   1.02155366e-01
-1.45929982e-02  -7.95205457e-02   5.59733152e-03  -3.58987179e-02
```

```
 7.16132260e-02   4.15425065e-02  -4.89180454e-02   1.65425755e-03
-6.48251747e-02   3.45951253e-02   5.32122058e-02  -1.28435276e-02
 1.48814403e-02  -6.49404547e-02  -6.01344770e-03   4.33784473e-02
-2.53362778e-04   3.81674519e-02  -4.83816002e-02  -2.53878079e-02
 1.96933442e-02  -3.04861682e-03   4.79203471e-02  -2.00930265e-02
-2.73895519e-02   3.30183589e-03  -1.67380508e-02   4.23917582e-02
 3.64690190e-03  -1.79916104e-02   7.31661649e-05  -2.99875575e-02
 2.71842526e-02   1.41806855e-02  -6.01781076e-03   5.86806100e-03
-3.32350597e-02   9.23347466e-03   1.47071722e-02  -7.42858080e-04
 1.63414270e-02  -2.87265671e-02  -1.64287280e-03   8.02601605e-03
-7.62613027e-04   2.18735533e-02  -1.78816282e-02  -6.58341101e-03
 2.67706547e-03  -6.25261247e-03   2.24942824e-02  -8.10756022e-03
-5.68160823e-03   7.01871209e-05  -1.15294332e-02   1.83608944e-02
-1.20567880e-03  -3.13147456e-03   1.39083675e-03  -1.49312478e-02
 1.32106694e-02   1.73474188e-03  -8.53469045e-04   4.03211203e-03
-1.55352991e-02   8.74711543e-03   1.93998895e-03  -2.71357322e-05
 6.13179585e-03  -1.41983972e-02   5.84710551e-03   9.22578333e-04
-2.16583469e-04   7.07919829e-03  -1.18488582e-02   4.39698322e-03
-8.91346785e-05  -3.42086367e-04   6.46355636e-03  -8.87555371e-03
 3.56799654e-03  -4.97335419e-04  -8.04560326e-04   5.55076717e-03
-7.13560569e-03   4.53679038e-03  -3.33261516e-03   2.35463427e-03
 2.04023789e-04  -1.27746711e-03   1.81247830e-04
```

The best nonnegative step function we are currently aware of, reaching the value $\|f * f\|_\infty = 1.50972...$, is attained at $n = 208$. The coefficients of its associate polynomial (a polynomial of degree 207 whose coefficients sum up to $\sqrt{416}$) are:

```
1.21174638  0.          0.          0.25997048  0.47606812
0.62295219  0.3296586   0.          0.29734381  0.
0.          0.          0.          0.          0.
0.          0.00846453  0.05731673  0.          0.13014906
0.          0.08357863  0.05268549  0.06456956  0.06158231
0.          0.          0.          0.          0.
0.          0.          0.          0.          0.
0.          0.          0.          0.          0.
0.          0.          0.          0.          0.
0.02396999  0.          0.          0.05846552  0.
0.          0.          0.          0.          0.0026332
0.0509835   0.          0.1283313   0.0904924   0.21232176
```

```
0.24866151  0.09933512  0.01963586  0.01363895  0.32389841
0.          0.          0.14467517  0.0129752   0.
0.          0.16299837  0.38329665  0.11361262  0.32074656
0.17344291  0.33181372  0.24357561  0.2577003   0.20567824
0.13085743  0.17116496  0.14349025  0.07019695  0.
0.          0.          0.          0.          0.
0.          0.          0.          0.          0.
0.          0.          0.          0.          0.
0.          0.0131741   0.0342541   0.0427565   0.03045044
0.07900079  0.07020678  0.08528342  0.09705597  0.0932896
0.09360206  0.06227754  0.07943462  0.08176106  0.10667185
0.10178412  0.11421821  0.07773213  0.11021377  0.12190377
0.06572457  0.07494855  0.          0.          0.02140202
0.          0.          0.0231478   0.00127997  0.
0.04672881  0.03886266  0.11141784  0.00695668  0.0466224
0.03543131  0.08803511  0.04165729  0.10785652  0.06747342
0.18785215  0.31908323  0.3249705   0.09824861  0.23309878
0.12428441  0.03200975  0.0933163   0.09527521  0.12202693
0.13179059  0.09266878  0.02013746  0.16448047  0.20324945
0.21810431  0.27321179  0.25242816  0.19993811  0.13683837
0.13304836  0.08794214  0.12893672  0.16904485  0.22510883
0.26079786  0.27367504  0.26271896  0.20457964  0.15073917
0.11014028  0.09896     0.0926069   0.13269111  0.17329988
0.20761774  0.21707182  0.18933169  0.14601258  0.08531506
0.06187865  0.06100211  0.09064962  0.12781018  0.17038096
0.185766    0.1734501   0.14667009  0.09569536  0.06092822
0.03219067  0.0495587   0.09657756  0.16382398  0.22606693
0.22230709  0.19833621  0.16155032  0.09330751  0.02838363
0.02769322  0.03349924  0.09448887  0.20517242  0.22849741
0.24175836  0.19700135  0.18168723
```

The best example of a step function disproving Conjecture 2 of [23], we are currently aware of, is attained for $n = 20$ (note that we did not make extensive efforts to optimize this example).

```
1.27283   0.54399   0.          0.          0.          0.
0.        0.529367  0.410195    0.46111     0.439352    0.448675
0.444699  0.446398  0.335601    0.322369    0.240811    0.202225
0.138305  0.0886248
```

This function reaches the value $c = 0.88922... > \frac{\log 16}{\pi}$ in equation (4.16).

Finally, the best step function we are currently aware of (which takes some negative values!), reaching the value $\|f * f\|_\infty = 1.45810...$, is attained at $n = 150$. The coefficients of its associate polynomial are:

```
 0.7506545   0.4648332   0.59759775  0.46028561  0.36666088
 0.37773841  0.16162776  0.3303943   0.15905831  0.08878588
 0.16284952 -0.09198076  0.05755583 -0.00690908 -0.08627636
-0.17180424 -0.14778207  0.13121791  0.05268415  0.20694965
 0.25287625  0.2071192  -0.13591836  0.05354584 -0.03558645
 0.15699341 -0.06508942 -0.01435246  0.02291645  0.18877783
-0.02751401  0.09592962  0.06666674  0.1807308   0.15543041
 0.02639022  0.01843893  0.04896963  0.0303207   0.05119754
 0.24099308  0.2244329   0.23689694  0.08980581  0.25272138
 0.26725296  0.12786816  0.16265063  0.20542404  0.06826679
 0.16905985 -0.11230055  0.26179213 -0.412312   -0.28820566
-0.7619902  -0.78933468  0.07066217  0.05785475  0.07163788
 0.09949514  0.0659708   0.05370837  0.08441868  0.10157278
 0.07317574  0.0521853   0.08980666  0.13113512  0.05943309
 0.07517572  0.12460218  0.14885796  0.09071907  0.13017884
 0.13185969  0.15196722  0.07848544  0.14924624  0.16053609
 0.17735544  0.14470971  0.17275872  0.16058981  0.22807136
 0.20728811  0.10876597  0.21471959  0.25136905  0.15147268
 0.06366331  0.05917714  0.05995267  0.35288009  0.3224057
 0.32988077  0.41806458  0.22880318  0.2080819   0.18504847
 0.27116284  0.16066195  0.02547032  0.26150045 -0.00634039
 0.09471136 -0.00407705  0.04759596 -0.07549638 -0.30815721
-0.00878173  0.08964445  0.23265916  0.37008611  0.18283593
 0.00240797  0.063899    0.02892268  0.10802879  0.15672677
-0.11335258  0.10549109  0.1571762   0.13290998 -0.01251118
 0.15487122  0.15770952  0.33037764  0.03888211  0.08105707
 0.00799348  0.00375632 -0.02392944  0.15019215  0.21615677
 0.17854093  0.04104506  0.12700956  0.23964236  0.05613369
 0.14857745  0.07375734  0.02816608  0.16226977  0.01757525
-0.23848002  0.05705152  0.29372066  0.56730329  1.105205
```

Appendix B

A sumset problem

Genius is one percent
inspiration, ninety-nine percent
perspiration.
Thomas Alva Edison

The work of this appendix is a joint work with Javier Cilleruelo and Manuel Silva [10].

Essentially, we prove that for a finite set of integers A, we always have $|A + 3 \cdot A| \geq 4|A| - 4$ (where $3 \cdot A = \{3 \cdot a,\ a \in A\}$) and we describe the cases of equality. We include the article as it will be published in *Journal of Combinatorics and Number Theory* in this appendix.

Abstract

We study the sumset $A + k \cdot A$ for the first non trivial case, $k = 3$, where $k \cdot A = \{k \cdot a,\ a \in A\}$. We prove that $|A + 3 \cdot A| \geq 4|A| - 4$ and that the equality holds only for $A = \{0, 1, 3\},\ A = \{0, 1, 4\},\ A = 3 \cdot \{0, \ldots, n\} \cup (3 \cdot \{0, \ldots, n\} + 1)$ and all the affine transforms of these sets.

B.1 Introduction

We address here the question of how large is the sumset $A + k \cdot A$ where $k \cdot A = \{k \cdot a,\ a \in A\}$ and A is a finite set of integers. It is well known that $|A + A| \geq 2|A| - 1$ and that equality only holds when A is an arithmetic progression. The case $k = 2$ (see [25]) can be studied easily by splitting A in the two residue classes modulo 2 and then obtaining $|A + 2 \cdot A| \geq 3|A| - 2$. It is not difficult to check that for any arithmetic progression with at least k elements, we have $|A + k \cdot A| = (k + 1)|A| - k$,

so it might be expected that arithmetic progressions are extremal cases for this problem, as when $k = 1$. Indeed this is the case for $k = 2$ as we will prove in Section B.2.

Theorem B.1.1. *For any set A we have $|A + 2 \cdot A| \geq 3|A| - 2$. Furthermore, if $|A + 2 \cdot A| = 3|A| - 2$, then A is an arithmetic progression or a singleton.*

For $k = 3$ Bukh [3] has proved in a recent paper that $|A + 3 \cdot A| \geq 4|A| - O(1)$ for any set A. Our main theorem gives, using a different argument, a sharp lower bound and a complete description of the extremal sets. We observe that these minimal sets for $k = 3$ are not arithmetic progressions anymore, as in the previous cases $k = 1, 2$. We observe also that the problem in consideration here is affine invariant.

Theorem B.1.2. *For any set A we have $|A + 3 \cdot A| \geq 4|A| - 4$. Furthermore if $|A + 3 \cdot A| = 4|A| - 4$ then $A = 3 \cdot \{0, \dots, n\} \cup (3 \cdot \{0, \dots, n\} + 1)$ or $A = \{0, 1, 3\}$ or $A = \{0, 1, 4\}$ or A is an affine transform of one of these sets.*

The general sums of dilated sets, $\lambda_1 \cdot A + \cdots + \lambda_k \cdot A$, have been studied by Bukh in [3]. The main theorem there says that for coprime integers $\lambda_1, \dots, \lambda_k$,

$$|\lambda_1 \cdot A + \cdots + \lambda_k \cdot A| \geq (|\lambda_1| + \cdots + |\lambda_k|)|A| - o(|A|).$$

In particular it gives $|A + k \cdot A| \geq (k + 1)|A| - o(|A|)$. As we will prove in Section B.5, there exist arbitrarily large sets A such that $|A + k \cdot A| = (k+1)|A| - \left\lceil \frac{k^2+2k}{4} \right\rceil$. We conjecture that this lower bound is sharp for large $|A|$.

B.2 Case $k = 2$ and preliminary lemmas

The next lemma is folklore, and we state it without proof.

Lemma B.2.1. *For arbitrary non empty finite sets A, B, we have*

i) $|A + B| \geq |A| + |B| - 1$.

ii) Furthermore, if equality holds, then A and B are arithmetic progressions with the same difference unless one of them is a singleton.

We generalize this lemma for any k. For that purpose, it is natural to divide A into residue classes modulo k. We define $\hat{A}$ to be the projection of A into $\mathbb{Z}/k\mathbb{Z}$.

Lemma B.2.2. *For arbitrary non empty sets B and $A = \bigcup_{i \in \hat{A}} (k \cdot A_i + i)$ we have*

i) $|A + k \cdot B| = \sum_{i \in \hat{A}} |A_i + B|$

ii) $|A + k \cdot B| \geq |A| + |\hat{A}|(|B| - 1)$.

iii) Furthermore, if equality holds in ii), then either $|B| = 1$ *or* $|A_i| = 1$ *for all* $i \in \hat{A}$ *or* B *and all the sets* A_i *with more than one element are arithmetic progressions with the same difference.*

Proof. For i) $|A + k \cdot B| = |\cup_{i \in \hat{A}} (k \cdot A_i + i + k \cdot B)| = \sum_{i \in \hat{A}} |k \cdot (A_i + B) + i| = \sum_{i \in \hat{A}} |A_i + B|$. To prove ii) we use i) and Lemma B.2.1-i). To prove iii) we observe that Lemma B.2.1-ii) implies that A_i and B are arithmetic progressions with the same difference except for the degenerate cases. □

Next we prove Theorem B.1.1 as a direct application of Lemma B.2.2.

Proof of Theorem B.1.1. If $|A| = 1$ then $|A + 2 \cdot A| = 3|A| - 2$, and these sets are described in Theorem B.1.1, so the inverse part is also proved.

So we assume $|A| \geq 2$. If $|\hat{A}| = 1$ then we can write $A = 2 \cdot A_i + i$ for some $i \in \{0, 1\}$ and $|A + 2 \cdot A| = |2 \cdot A_i + i + 4 \cdot A_i + 2i| = |A_i + 2 \cdot A_i|$. Now, if $|\hat{A}_i| = 1$, we can repeat this process and it is clear that we will eventually obtain a set A' with $|\hat{A}'| = 2$ (since it cannot be greater for $k = 2$) that is an affine transformation of the set A.

Thus we can also assume that $|\hat{A}| = 2$. By Lemma B.2.2-ii) we conclude that $|A + 2 \cdot A| \geq |A| + 2(|A| - 1) = 3|A| - 2$. For the inverse part, if the equality holds, Lemma B.2.2-iii) implies that either $|A| = 1$ or $|A_0| = |A_1| = 1$ or A is an arithmetic progression. We finish by observing that $|A| = 1$ is impossible since we assumed $|A| \geq 2$ and $|A_0| = |A_1| = 1$ implies that $|A| = 2$, so it is an arithmetic progression. □

For the case $k = 3$ we will need some preliminary lemmas. In the rest of this section and in the next one, k will be equal to 3 and so $\hat{A}$ will always be the projection of A into $\mathbb{Z}/3\mathbb{Z}$.

Lemma B.2.3. *If* $A = 3 \cdot A_0 \cup (3 \cdot A_1 + 1)$ *with* A_0 *and* A_1 *non empty sets, then*

i) $|A + 3 \cdot A| \geq |A_0 + 3 \cdot A_0| + |A_1 + 3 \cdot A_1| + 2$.

ii) $|A + 3 \cdot A| \geq |A_0 + 3 \cdot A_1| + |A_1 + 3 \cdot A_0| + 2$.

Proof. To prove i) we write

$$|A + 3 \cdot A| \quad = \quad |A_0 + A| + |A_1 + A|$$

$$\begin{aligned} &= |(A_0 + 3\cdot A_0) \cup (A_0 + 3\cdot A_1 + 1)| \\ &\quad +|(A_1 + 3\cdot A_0) \cup (A_1 + 3\cdot A_1 + 1)| \\ &= |A_0 + 3\cdot A_0| + |A_1 + 3\cdot A_1 + 1| \\ &\quad +|(A_0 + 3\cdot A_1 + 1) \setminus (A_0 + 3\cdot A_0)| \\ &\quad +|(A_1 + 3\cdot A_0) \setminus (A_1 + 3\cdot A_1 + 1)| \end{aligned}$$

Then we only need to check that the last line above is at least 2. If $|A_0| = 1$ and $|A_1| = 1$, we write $A_0 = \{a_0\}$ and $A_1 = \{a_1\}$. Then $a_0 + 3a_1 + 1 \neq a_0 + 3a_0$ and $a_1 + 3a_0 \neq a_1 + 3a_1 + 1$ because they are different modulo 3, so we have two extra elements. If not, let m_i and M_i be the minimum and the maximum of $A_i,\ i = 0, 1$, and we know that for at least one i, $m_i \neq M_i$.

If $M_0 \leq M_1$ then $M_0 + 3M_1 + 1 \in (A_0 + 3\cdot A_1 + 1) \setminus (A_0 + 3\cdot A_0)$ because $M_0 + 3M_1 + 1$ is greater than $M_0 + 3M_0$, which is the maximum of $A_0 + 3\cdot A_0$. On the other hand, if $M_0 > M_1$, then $M_1 + 3M_0 \in (A_1 + 3\cdot A_0) \setminus (A_1 + 3\cdot A_1 + 1)$.

If $m_0 \leq m_1$ then $m_1 + 3m_0 \in (A_1 + 3\cdot A_0) \setminus (A_1 + 3\cdot A_1 + 1)$ and if $m_0 > m_1$ then $m_0 + 3m_1 + 1 \in (A_0 + 3\cdot A_1 + 1) \setminus (A_0 + 3\cdot A_0)$.

We obtain one extra element in each case. To see that the elements in the same set are distinct, observe that if $M_0 + 3M_1 + 1 = m_0 + 3m_1 + 1$, then we must have $M_0 = m_0$ and $M_1 = m_1$, a contradiction. The same thing happens if $M_1 + 3M_0 = m_1 + 3m_0$. The proof of ii) is similar. □

Lemma B.2.4. *If $A = 3\cdot A_0 \cup (3\cdot A_1 + 1)$ with A_0 and A_1 non empty sets, then*

i) If $|\hat{A}_0| = 2$, we have $|A_0 + A| \geq 2|A| - 2$.

ii)
- *If $|\hat{A}_0| \leq 2$ and $|A_0 + 3\cdot A_0| \geq 4|A_0| - 4$, we have $|A_0 + A| \geq 4|A_0| + |A_1| - 4$.*
- *If $|\hat{A}_1| \leq 2$ and $|A_1 + 3\cdot A_1| \geq 4|A_1| - 4$, we have $|A_1 + A| \geq 4|A_1| + |A_0| - 4$.*

Proof. For i), let $\hat{A}_0 = \{u, u+1\}$. We can write $A_0 = A_0^u \cup A_0^{u+1}$, where $A_0^u = \{x \in A_0,\ x \equiv u \pmod 3\}$. Then

$$\begin{aligned} |A_0 + A| &= |(A_0 + 3\cdot A_0) \cup (A_0 + 3\cdot A_1 + 1)| \\ &= |(A_0^u + 3\cdot A_0) \cup (A_0^{u+1} + 3\cdot A_0) \cup (A_0^u + 3\cdot A_1 + 1) \\ &\quad \cup (A_0^{u+1} + 3\cdot A_1 + 1)| \\ &\geq |A_0^u + 3\cdot A_0| + |A_0^u + 3\cdot A_1 + 1| + |A_0^{u+1} + 3\cdot A_1 + 1| \\ &\geq |A_0^u| + |A_0| - 1 + |A_1| + |A_0^{u+1}| + |A_1| - 1 = 2|A| - 2, \end{aligned}$$

where we have used Lemma B.2.1-i) twice.

For part ii), we again write $A_0 = A_0^u \cup A_0^{u+1}$ if $|\hat{A}_0| = 2$, or $A_0 = A_0^{u+1}$ if $|\hat{A}_0| = 1$. Then

$$\begin{aligned} |A_0 + A| &= |(A_0 + 3 \cdot A_0) \cup (A_0 + 3 \cdot A_1 + 1)| \\ &\geq |(A_0 + 3 \cdot A_0) \cup (A_0^{u+1} + 3 \cdot A_1 + 1)| \\ &= |A_0 + 3 \cdot A_0| + |A_0^{u+1} + 3 \cdot A_1 + 1| \\ &\geq 4|A_0| - 4 + |A_1|. \end{aligned}$$

The same argument works for A_1 instead of A_0. □

Lemma B.2.5.

i) If $|A| = 2$ *then* $|A + 3 \cdot A| = 4|A| - 4 = 4$.

ii) If $|A| = 3$ *then* $|A+3\cdot A| \geq 4|A|-4$. *Furthermore, if* $|A| = 3$ *and* $|A+3\cdot A| = 4|A| - 4$ *then* A *is an affine transform of* $\{0, 1, 3\}$ *or* $\{0, 1, 4\}$.

Proof. i) By an affine transformation we may assume $A = \{0, 1\}$. Then $A+3\cdot A = \{0, 1, 3, 4\}$.

ii) By an affine transformation we may assume that $A = \{0, 1, a\}$, where $a > 1$ is a rational number. We have that

$$A + 3 \cdot A = \{0, 1, a, 3, 4, 3 + a, 3a, 3a + 1, 4a\}.$$

If $A + 3 \cdot A$ has 8 or less elements then there is some repeated element in the sumset. The possible repetitions come from $a = 3$, $a = 4$, $4 = 3a$, $3 + a = 3a$ which provide the sets $\{0, 1, 3\}$, $\{0, 1, 4\}$, $\{0, 3, 4\}$, $\{0, 2, 3\}$. All these sets have $|A + 3 \cdot A| = 8 = 4|A| - 4$. □

B.3 Proof of Theorem B.1.2: the inequality

In this section, we will prove the lower bound in Theorem B.1.2 for $|A + 3 \cdot A|$. That is, we will prove that for every set A, we have $|A + 3 \cdot A| \geq 4|A| - 4$. In the next section, we will prove the inverse part which is more involved.

We distinguish three cases according to the different values of $|\hat{A}|$.

If $|\hat{A}| = 3$ then (by Lemma B.2.2-ii)) we have that $|A + 3 \cdot A| \geq 4|A| - 3$, a better lower bound than that we want to prove in Theorem B.1.2.

If $|\hat{A}| = 1$ and $|A| = 1$, then $4|A| - 4 = 0$ and the theorem is trivial. If $|\hat{A}| = 1$ and $|A| > 1$, then we write $A = 3 \cdot A_i + i$ and we have $|A + 3 \cdot A| = |A_i + 3 \cdot A_i|$. If $|\hat{A}_i| = 1$, we repeat the process with A replaced by A_i until we find a set with $|\hat{A}_i|$ equal to 2 or 3. Cardinality 3 has been treated above.

So we can now assume that $|\hat{A}| = 2$ and write $A = (3 \cdot A_i + i) \cup (3 \cdot A_{i+1} + i + 1)$. We can assume that $|\hat{A}_i| \leq |\hat{A}_{i+1}|$. If not the set $B = -A$ could be written as $B = (3 \cdot B_j + j) \cup (3 \cdot B_{j+1} + j + 1)$ where $B_j = -A_{i+1} - 1$, $B_{j+1} = -A_i - 1$, $j = 2 - i$, and in this case we would have $|\hat{B}_j| \leq |\hat{B}_{j+1}|$. Finally, by translation we can assume

- $A = 3 \cdot A_0 \cup (3 \cdot A_1 + 1)$
- $\min A_0 = 0$
- $|\hat{A}_0| \leq |\hat{A}_1|$.

Assuming all this, we prove $|A + 3 \cdot A| \geq 4|A| - 4$ by induction on $|A|$. The inequality clearly holds for $|A| = 1$. Suppose we have proved it for any set with fewer elements than A, in particular for A_0 and A_1. We distinguish three cases:

Case $|\hat{A}_0| = |\hat{A}_1| = 3$. We use Lemma B.2.3-i) and Lemma B.2.2-ii) to obtain

$$|A + 3 \cdot A| \geq |A_0 + 3 \cdot A_0| + |A_1 + 3 \cdot A_1| + 2 \geq 4|A_0| - 3 + 4|A_1| - 3 + 2 = 4|A| - 4.$$

Case $|\hat{A}_1| = 3$, $|\hat{A}_0| < 3$. We apply Lemma B.2.4-ii) (using the induction hypothesis) and Lemma B.2.2-ii) to obtain

$$\begin{aligned} |A + 3 \cdot A| &= |A_0 + A| + |A_1 + A| \geq |A_0 + A| + |A_1 + 3 \cdot A_1| \\ &\geq 4|A_0| + |A_1| - 4 + 4|A_1| - 3 = 4|A| - 4 + |A_1| - 3 \\ &\geq 4|A| - 4. \end{aligned}$$

In the last inequality we have used that $|A_1| \geq |\hat{A}_1| = 3$.

Case $|\hat{A}_1| < 3$. We apply Lemma B.2.4-ii) to A_0 and A_1 (again, using the induction hypothesis) to obtain

$$|A+3\cdot A| = |A_0+A|+|A_1+A| \geq 4|A_0|+|A_1|-4+4|A_1|+|A_0|-4 = 4|A|-4+|A|-4.$$

If $|A| \geq 4$ this gives the bound. If not, we use Lemma B.2.5. This completes the proof.

B.4 Proof of Theorem B.1.2: the cases of equality

Now we turn to the proof of the inverse part of Theorem B.1.2. Once we know that $|A+3\cdot A|\geq 4|A|-4$ for every set - and also we have some examples where the equality holds (see Lemma B.2.5) - we characterize all the sets that satisfy the equality $|A+3\cdot A|=4|A|-4$.

As in the previous section we can assume $A=3\cdot A_0\cup(3\cdot A_1+1)$, $|\hat{A}_0|\leq|\hat{A}_1|$ and $\min A_0=0$.

Case $|\hat{A}_0|=|\hat{A}_1|=3$**.** We use Lemma B.2.3-i) and B.2.3-ii) and Lemma B.2.2-ii) to obtain

$$\begin{aligned} 4|A|-4 &= |A+3\cdot A|\geq |A_0+3\cdot A_0|+|A_1+3\cdot A_1|+2\\ &\geq |A_0|+3|A_0|-3+|A_1|+3|A_1|-3+2=4|A|-4. \end{aligned}$$

and

$$\begin{aligned} 4|A|-4 &= |A+3\cdot A|\geq |A_0+3\cdot A_1|+|A_1+3\cdot A_0|+2\\ &\geq |A_0|+3|A_1|-3+|A_1|+3|A_0|-3+2=4|A|-4. \end{aligned}$$

Then, the inequalities are, indeed, equalities. So $|A_0+3\cdot A_0|=|A_0|+3|A_0|-3$, $|A_1+3\cdot A_1|=|A_1|+3|A_1|-3$, $|A_0+3\cdot A_1|=|A_0|+3|A_1|-3$ and $|A_1+3\cdot A_0|=|A_1|+3|A_0|-3$. Now we apply Lemma B.2.2-iii) to conclude that (since $|A_0|\geq|\hat{A}_0|=3$ and $|A_1|\geq|\hat{A}_1|=3$)

a) either $A_0=\{x_0,x_1,x_2\}$ and $A_1=\{y_0,y_1,y_2\}$ with $x_i,y_i\equiv i \pmod 3$

b) or A_0 and A_1 are arithmetic progressions with the same difference, d.

a) In this subcase, $|A|=6$ and $4|A|-4=20$, and we know by Lemma B.2.2-i) that $20=|A+3\cdot A|=|A_0+A|+|A_1+A|$. Then, $|A_0+A|\leq 10$ or $|A_1+A|\leq 10$. We suppose that $|A_0+A|\leq 10$ (the other case is identical) and, because $A_0=\{x_0,x_1,x_2\}$ with $x_i\equiv i \pmod 3$, we have

$$\begin{aligned} 10 &\geq |(A_0+3\cdot A_0)\cup(A_0+3\cdot A_1+1)|\\ &= |(x_0+3\cdot A_0)\cup(x_2+3\cdot A_1+1)|\\ &\quad +|(x_1+3\cdot A_0)\cup(x_0+3\cdot A_1+1)|\\ &\quad +|(x_2+3\cdot A_0)\cup(x_1+3\cdot A_1+1)| \end{aligned}$$

$$
\begin{aligned}
= \quad & \left|A_0 \cup \left(A_1 + \frac{x_2 - x_0 + 1}{3}\right)\right| \\
& + \left|A_0 \cup \left(A_1 + \frac{x_0 - x_1 + 1}{3}\right)\right| \\
& + \left|A_0 \cup \left(A_1 + \frac{x_1 - x_2 + 1}{3}\right)\right|
\end{aligned}
$$

and we can observe that each addend gives us at least 4 elements unless the two members of the union are equal (in this case we have only 3 elements). But, because the sum of the three addends is less than or equal to 10, we must have at least two equalities, for example:

$$A_0 = A_1 + \frac{x_2 - x_0 + 1}{3} \text{ and } \; A_0 = A_1 + \frac{x_0 - x_1 + 1}{3}.$$

Then, we have $x_2 - x_0 = x_0 - x_1$, so A_0 is an arithmetic progression and also A_1 is an arithmetic progression with the same difference, since it is a translation of A_0. The other possibilities are identical.

b) In this case both A_0 and A_1 are arithmetic progressions with difference d, and because $\min A_0 = 0$ we can write $A_0 = d\cdot[0, n_0-1]$, $A_1 = d\cdot[0, n_1-1]+e$. Since $n_0, n_1 \geq 3$, we have that $[0, n_i - 1] + 3 \cdot [0, n_j - 1] = [0, 3n_j + n_i - 4]$ for any $i, j \in \{0, 1\}$. Thus

$$
\begin{aligned}
|A + 3 \cdot A| &= |A_0 + A| + |A_1 + A| \\
&= |d \cdot ([0, n_0 - 1] + 3 \cdot [0, n_0 - 1]) \\
&\quad \cup (d \cdot ([0, n_0 - 1] + 3 \cdot [0, n_1 - 1]) + 3e + 1)| \\
&\quad + |(d \cdot ([0, n_1 - 1] + 3 \cdot [0, n_0 - 1]) + e) \\
&\quad \cup (d \cdot ([0, n_1 - 1] + 3 \cdot [0, n_1 - 1]) + 4e + 1)| \\
&= |d \cdot [0, 4n_0 - 4] \cup (d \cdot [0, 3n_1 + n_0 - 4] + 3e + 1)| \\
&\quad + |d \cdot [0, 4n_1 - 4] \cup (d \cdot [0, 3n_0 + n_1 - 4] - 3e - 1)|.
\end{aligned}
$$

If $n_1 > n_0$ then

$$
\begin{aligned}
|A + 3 \cdot A| &\geq 3n_1 + n_0 - 3 + 4n_1 - 3 = 4(n_0 + n_1) + 3(n_1 - n_0) - 6 \\
&\geq 4|A| - 3,
\end{aligned}
$$

which is a contradiction. So $n_1 \leq n_0$. For the same reason (interchanging n_0

and n_1) we have that $n_0 \leq n_1$ and then $n_0 = n_1$. Now we can write

$$\begin{aligned} |A + 3 \cdot A| &= |d \cdot [0, 4n_0 - 4] \cup (d \cdot [0, 4n_0 - 4] + 3e + 1)| \\ &+ |d \cdot [0, 4n_0 - 4] \cup (d \cdot [0, 4n_0 - 4] - 3e - 1)|. \end{aligned}$$

If $3e + 1 \not\equiv 0 \pmod{d}$ then the unions are disjoint and we have $4|A| - 4 = |A + 3 \cdot A| = 2(4n_0 - 3) + 2(4n_0 - 3) = 8|A| - 12$. That implies that $|A| = 2$ and this is impossible since $|A| = |A_0| + |A_1| \geq |\hat{A}_0| + |\hat{A}_1| = 6$. If $3e + 1 \equiv 0 \pmod{d}$ we write $3e + 1 = de'$ and then

$$\begin{aligned} |A + 3 \cdot A| &= |[0, 4n_0 - 4] \cup ([0, 4n_0 - 4] + e')| \\ &+ |[0, 4n_0 - 4] \cup ([0, 4n_0 - 4] - e')|. \end{aligned}$$

If $|e'| \geq 2$ then the cardinality of each union is greater than or equal to $4n_0 - 1$, and $|A + 3 \cdot A| \geq 4n_0 - 1 + 4n_0 - 1 = 4|A| - 2$. So, since $e' \neq 0$ (remember that de' is an integer different from 0) then $e' = \pm 1$, so $3e + 1 = \pm d$ and $A = 3 \cdot A_0 \cup 3 \cdot A_1 + 1 = d \cdot (3 \cdot [0, n_0 - 1] \cup 3 \cdot [0, n_0 - 1] \pm 1)$. These sets are listed as extremal sets in Theorem B.1.2.

Case $|\hat{A}_0| = 2,\ |\hat{A}_1| = 3$**.** We write

$$|A_1 + A| = |(A_1 + 3 \cdot A_0) \cup (A_1 + 3 \cdot A_1 + 1)| = |A_1 + 3 \cdot A_1| + |(A_1 + 3 \cdot A_0) \setminus (A_1 + 3 \cdot A_1 + 1)|.$$

Lemma B.2.2-i), Lemma B.2.4-ii) and the equality above imply that

$$\begin{aligned} |A + 3 \cdot A| &= |A_0 + A| + |A_1 + A| \\ &\geq 4|A_0| + |A_1| - 4 + 4|A_1| - 3 + (|A_1 + 3 \cdot A_1| - 4|A_1| + 3) \\ &+ |(A_1 + 3 \cdot A_0) \setminus (A_1 + 3 \cdot A_1 + 1)|. \end{aligned}$$

Then

$$\begin{aligned} 4|A| - 4 = |A + 3 \cdot A| \geq\ & 4|A| - 4 + (|A_1| - 3) + (|A_1 + 3 \cdot A_1| - 4|A_1| + 3) \\ & + |(A_1 + 3 \cdot A_0) \setminus (A_1 + 3 \cdot A_1 + 1)|. \end{aligned}$$

Using that $|A_1| \geq |\hat{A}_1| = 3$ and Lemma B.2.2-ii) we see that the three last addends are non negative. But the inequality implies that all of them are indeed 0. Then,

i) $|A_1| = 3$.

ii) By Lemma B.2.2-iii),

a) either $A_1 = \{y_0, y_1, y_2\}$ with $y_i \equiv i \pmod 3$

b) or A_1 is an arithmetic progression, say $A_1 = d \cdot [0,2] + e$.

iii) $3 \cdot A_0 \subseteq A_1 - A_1 + 3 \cdot A_1 + 1$ (because $A_1 + 3 \cdot A_0 \subset A_1 + 3 \cdot A_1 + 1$).

Now we claim that also $|A_0| = 3$. To see that we will obtain a lower and an upper bound.

To prove $|A_0| \leq 3$ we use Lemma B.2.2-i), Lemma B.2.4-ii), Lemma B.2.2-ii) and the fact that $|A_1| = 3$ to have

$$\begin{aligned} |A + 3 \cdot A| &= |A_0 + A| + |A_1 + A| \geq |A_0 + A| + |A_1 + 3 \cdot A_0| \geq \\ & 4|A_0| + |A_1| - 4 + |A_1| + 3(|A_0| - 1) = 4|A| - 4 + 3|A_0| - 9. \end{aligned}$$

Since we have assumed that $|A + 3 \cdot A| = 4|A| - 4$ then $|A_0| \leq 3$.

To prove $|A_0| \geq 3$ we use Lemma B.2.2-i), Lemma B.2.4-i) and Lemma B.2.5-ii) (for a set A of three elements that covers the three classes modulo 3 we must have $|A + 3 \cdot A| = 9$) to obtain

$$4|A| - 4 = |A + 3 \cdot A| = |A_0 + A| + |A_1 + A| \geq 2|A| - 2 + |A_1 + 3 \cdot A_1| = 2|A| - 2 + 9,$$

so $|A| \geq 11/2$. And since $|A_1| = 3$ we have that $|A_0| \geq 5/2$, so $|A_0| \geq 3$.

So we have proved that $|A| = 6$.

Next we will see that if we are in case ii)-a), that is if $A_1 = \{y_0, y_1, y_2\}$ with $y_i \equiv i \pmod 3$, then A_1 is an arithmetic progression. As in a) of the case $|\hat{A}_0| = |\hat{A}_1| = 3$ we have, $20 = 4|A| - 4 = |A + 3 \cdot A| = |A_0 + A| + |A_1 + A|$. Again, one of them is less or equal than 10. If $|A_1 + A| \leq 10$ then we proceed exactly as we did in that case and we have that A_1 is an arithmetic progression. If $|A_0 + A| \leq 10$ then $A_0 = \{x_0, y_0, x_1\}$ or $A_0 = \{x_0, y_0, x_2\}$ where $x_i \equiv y_i \equiv i \pmod 3$ except for translations. In the first case $10 \geq |A_0 + A| = |(A_0 + 3 \cdot A_0) \cup (A_0 + 3 \cdot A_1 + 1)| \geq |(x_0 + 3 \cdot A_0) \cup (y_0 + 3 \cdot A_0)| + |(x_0 + 3 \cdot A_1 + 1) \cup (y_0 + 3 \cdot A_1 + 1)| + |x_1 + 3 \cdot A_1 + 1| \geq 4 + 4 + 3 = 11$, which is a contradiction. The second case is similar.

Thus, the only possibility is ii)-b), that is, A_1 is an arithmetic progression, say $A_1 = d \cdot [0,2] + e$, and then $A_1 + 3 \cdot A_1 + 1 - A_1 = d \cdot [-2,8] + 3e + 1$, so by iii) we have that

$$3 \cdot A_0 \subseteq d \cdot [-2,8] + 3e + 1. \tag{B.1}$$

Inclusion (B.1) implies that $(d, 3) = 1$.

Suppose $d \equiv 1 \pmod 3$. Then $3 \cdot A_0 \subseteq d \cdot \{-1,2,5,8\} + 3e + 1$. In this case $A = d \cdot (S \cup \{0,3,6\}) + 3e + 1$, where $S = \{-1,2,8\}$ or $S = \{-1,5,8\}$. Observe that these sets are the only subsets of three elements of $\{-1,2,5,8\}$ satisfying that $|\widehat{\frac{1}{3}(S+1)}| = 2$. Since the problem is invariant by translations and dilations we only have to check the sets $A = \{-1,0,2,3,6,8\}$ and $A = \{-1,0,3,5,6,8\}$.

If $d \equiv 2 \pmod 3$ the sets we have to check are $A = \{-2,0,1,3,6,7\}$ and $A = \{-2,0,3,4,6,7\}$. The four sets we have described satisfy $|A+3\cdot A| = 24 \neq 4|A|-4$.

Case $|\hat{A}_0| = 1,\ |\hat{A}_1| = 3$. Since $|\hat{A}_0| = 1$ we have $|A_0+A| = |(A_0+3\cdot A_0)\cup(A_0+3\cdot A_1+1)| = |A_0+3\cdot A_0|+|A_0+3\cdot A_1| \geq 4|A_0|-4+|A_0|+|A_1|-1 = 5|A_0|+|A_1|-5$. Also we have that $|A_1 + A| \geq |A_1 + 3 \cdot A_1| \geq 4|A_1| - 3$. Then

$$4|A|-4 = |A+3\cdot A| = |A_0+A|+|A_1+A| \geq 5|A_0|+|A_1|-5+4|A_1|-3 = 5|A|-8,$$

thus $|A| \leq 4$. But since $|\hat{A}_0| = 1$ and $|\hat{A}_1| = 3$ we have that $|A_0| = 1$ and $|A_1| = 3$. In this case we get $|A_0 + A| = |A_0 + 3 \cdot A_0| + |A_0 + 3 \cdot A_1| = 1 + |A_1| = 4$. Then

$$12 = 4|A| - 4 = |A + 3 \cdot A| = |A_0 + A| + |A_1 + A| \geq 4 + 4|A_1| - 3 = 13$$

and we get a contradiction.

Case $|\hat{A}_0| = 2,\ |\hat{A}_1| = 2$. We can write, as in the proof of Lemma B.2.4, $A_0 = A_0^u \cup A_0^{u+1}$ and $A_1 = A_1^v \cup A_1^{v+1}$, where $A_i^j = \{x \in A_i,\ x \equiv j \pmod 3\}$.

$$|A_0 + A| \geq |A_0 + 3 \cdot A_0| + |A_0^{u+1} + 3 \cdot A_1 + 1| \geq 4|A_0| - 4 + |A_1|.$$

Similary $|A_1+A| \geq 4|A_1|-4+|A_0|$. Then $4|A|-4 = |A+3\cdot A| = |A_0+A|+|A_1+A| \geq 4|A_0|-4+|A_1|+4|A_1|-4+|A_0| = 5|A|-8$ and thus $|A| \leq 4$. Since $|\hat{A}_0| = |\hat{A}_1| = 2$ we have that $|A_0| = |A_1| = 2$. Write $A_0 = \{a_0, b_0\},\ A_1 = \{a_1, b_1\}$ with $b_i \equiv a_i + 1 \pmod 3,\ i = 0, 1$, and

$$\begin{aligned}
|A_0 + A| &= |a_0 + 3 \cdot A_0| + |(b_0 + 3 \cdot A_0) \cup (a_0 + 1 + 3 \cdot A_1)| + |b_0 + 1 + 3 \cdot A_1| \\
&\geq 4 + |3 \cdot A_0 \cup (a_0 - b_0 + 1 + 3 \cdot A_1)|, \\
|A_1 + A| &= |a_1 + 3 \cdot A_0| + |(b_1 + 3 \cdot A_0) \cup (a_1 + 1 + 3 \cdot A_1)| + |b_1 + 1 + 3 \cdot A_1| \\
&\geq 4 + |3 \cdot A_0 \cup (a_1 - b_1 + 1 + 3 \cdot A_1)|.
\end{aligned}$$

Hence

$$12 = 4|A| - 4 = |A + 3 \cdot A| = |A_0 + A| + |A_1 + A|$$

$$\geq \quad 8 + |3 \cdot A_0 \cup (a_0 - b_0 + 1 + 3 \cdot A_1)| + |3 \cdot A_0 \cup (a_1 - b_1 + 1 + 3 \cdot A_1)|.$$

We claim that $3 \cdot A_0 = a_1 - b_1 + 1 + 3 \cdot A_1$. Otherwise we would obtain more than 2 elements in the last sum and we would get a contradiction. Then $3 \cdot A_0 = \{3a_1 + a_1 - b_1 + 1, 3b_1 + a_1 - b_1 + 1\} = \{4a_1 - b_1 + 1, a_1 + 2b_1 + 1\}$, so we obtain a set A described in Theorem B.1.2,

$$\begin{aligned} A &= 3 \cdot A_0 \cup (3 \cdot A_1 + 1) = \{4a_1 - b_1, a_1 + 2b_1, 3a_1, 3b_1\} + 1 \\ &= 3b_1 + 1 + (a_1 - b_1) \cdot \{0, 1, 3, 4\}. \end{aligned}$$

Case $|\hat{A}_0| = 1,\ |\hat{A}_1| = 2$**.** In this case we have

$$|A_0 + A| = |A_0 + 3 \cdot A_0| + |A_0 + 3 \cdot A_1| \geq 4|A_0| - 4 + |A_0| + |A_1| - 1 = 5|A_0| + |A_1| - 5$$

and we apply Lemma B.2.4-ii) to obtain $|A_1 + A| \geq 4|A_1| + |A_0| - 4$. Then

$$4(|A_0| + |A_1|) - 4 = |A + 3 \cdot A| = |A_0 + A| + |A_1 + A| \geq 5|A_0| + |A_1| - 5 + 4|A_1| + |A_0| - 4,$$

so $5 \geq 2|A_0| + |A_1|$. Since $|\hat{A}_1| = 2$ then $|A_1| \geq 2$ and $|A_0| \leq 3/2$; so $|A_0| = 1$. But in this case we have that $|A_0 + A| = |A|$ and $|A_1 + A| \geq 4|A_1| - 3$. Then $4|A_1| = 4|A| - 4 \geq |A| + 4|A_1| - 3$, so $|A| \leq 3$. Indeed, since $|\hat{A}_1| = 2$ and $|\hat{A}_0| = 1$ we have that $|A| = 3$. These cases are analyzed in Lemma B.2.5.

Case $|\hat{A}_0| = 1,\ |\hat{A}_1| = 1$**.** As above we have $|A_0 + A| \geq 5|A_0| + |A_1| - 5$ and also we have $|A_1 + A| \geq 5|A_1| + |A_0| - 5$. Then $4|A| - 4 = |A + 3 \cdot A| = |A_0 + A| + |A_1 + A| \geq 6|A| - 10$, so $|A| \leq 3$ and the result again follows from Lemma B.2.5.

B.5 Small sumsets $A + k \cdot A$

Now we show some constructions that give a small sumset, $A + k \cdot A$, for general $k \in \mathbb{N}$.

Proposition B.5.1. *For any $k \in \mathbb{Z}_{>0}$*

i) there exist arbitrarily large sets A such that

$$|A + k \cdot A| = (k+1)|A| - \left\lceil \frac{k^2 + 2k}{4} \right\rceil$$

ii) there exists a set A such that

$$|A + k \cdot A| = (k+1)|A| - \frac{k^3 + 6k^2 + 9k + \delta_k}{27}$$

where

$$\delta_k = \begin{cases} 3k+8 & \text{if } k \equiv 1 \pmod 3 \\ 4 & \text{if } k \equiv 2 \pmod 3 \\ 0 & \text{if } k \equiv 0 \pmod 3 \end{cases}.$$

We conjecture that, for a fixed k, the constructions given in i) are the best possible, in the sense that for a large set A we always have $|A + k \cdot A| \geq (k+1)|A| - \left\lceil \frac{k^2+2k}{4} \right\rceil$. But the construction given in ii) says that there are small sets that achieve a smaller lower bound.

Proof. Following the examples we obtained in the inverse problem for k=3, we consider sets that are unions of arithmetic progressions with difference k. We write

$$A = \bigcup_{i \in I} (k \cdot [0, m-1] + i)$$

where I is an interval, $I = [0, |I| - 1] \subseteq [0, k-1]$. Then $|A| = |I|m$. As in Lemma B.2.2, we have (with $A_i = [0, m-1]$ for all i)

$$|A + k \cdot A| = \sum_{i \in I} |A_i + A|.$$

and

$$A_i + A = [0, m-1] + \bigcup_{i \in I} (k \cdot [0, m-1] + i) = [0, m-1] + k \cdot [0, m-1] + I.$$

Now, we try to find the sets of this shape that give us the smallest sumset, $A + k \cdot A$.

i) If $m \geq k$

$$A_i + A = [0, (k+1)(m-1) + |I| - 1]$$

so

$$|A + k \cdot A| = |I|((k+1)(m-1) + |I|) = (k+1)|A| - |I|(k + 1 - |I|).$$

We want to maximize $|I|(k+1-|I|)$ in order to get an A with small sumset.

If we think of $|I|$ as a real number we can look at the derivative to see that this happens when $|I| = \frac{k+1}{2}$. If k is odd everything works and if k is even we take $|I| = \frac{k}{2}$ or $|I| = \frac{k+2}{2}$ and in any case we have the formula of the proposition.

ii) If $0 < m < k$, then $A_i + A$ is the union of m intervals of lenght $m + |I| - 1$ starting on $0, k, 2k, \ldots$ and $(m-1)k$. If we do not want this intervals to overlap, then we must impose $m + |I| - 1 \leq k$, i. e. $|I| \leq k + 1 - m$. Then

$$|A_i + A| = (m + |I| - 1)m$$

and

$$|A + k \cdot A| = |I|m(m + |I| - 1) = (k+1)|A| - m|I|(k + 2 - m - |I|).$$

We want to maximize $m|I|(k + 2 - m - |I|)$. If we think of m and $|I|$ as real numbers, we can look at the gradient to conclude that the maximum occurs for $m = |I| = \frac{k+2}{3}$. If $k \equiv 1\ (3)$, everything works and we have $|A + k \cdot A| = (k+1)|A| - \left(\frac{k+2}{3}\right)^3$ as in ii) of the theorem. If $k \equiv 2\ (3)$, we can take $m = |I| = \frac{k+1}{3}$ or one of them equal to $\frac{k+1}{3}$ and the other to $\frac{k+4}{3}$ and we have $|A + k \cdot A| = (k+1)|A| - \left(\frac{k+1}{3}\right)^2 \left(\frac{k+4}{3}\right)$. Finally, if $k \equiv 0\ (3)$, we take $m = |I| = \frac{k+3}{3}$ or one equal to $\frac{k+3}{3}$ and the other to $\frac{k}{3}$ and we have $|A + k \cdot A| = (k+1)|A| - \left(\frac{k+3}{3}\right)^2 \left(\frac{k}{3}\right)$. This proves ii).

□

✎ This thesis was finished on October 30th, 2009
in Madrid.